T2S FRAMEWORK AGREEMENT

BETWEEN

[• INSERT THE NAME OF THE ACTING EURO AREA NCB/ECB]

ACTING IN THE NAME AND ON BEHALF OF ALL OF THE MEMBERS OF THE EUROSYSTEM

AND

[• INSERT THE NAME OF THE CONTRACTING CSD]
T2S Framework Agreement

TABLE OF CONTENTS

LIST OF SCHEDULES

PREAMBLE

CHAPTER 1  SCOPE, DEFINITIONS AND CONSTRUCTION

Article 1  Scope
Article 2  Definitions and construction

CHAPTER 2  RIGHTS AND OBLIGATIONS OF THE PARTIES

Article 3  Representations of the Parties
Article 4  Multilateral Character of T2S
Article 5  Non-discriminatory access
Article 6  Duty of loyal cooperation and information
Article 7  Assignment and subcontracting
Article 8  Compliance with Legal and Regulatory Requirements, separation of functions
Article 9  Availability of expert personnel
Article 10  Compliance with Information Security requirements
Article 11 T2S Network Service Provider
Article 12 Directly Connected Parties
Article 13 Obligations of the Eurosystem related to the development of the T2S
Article 14 Obligations of the Contracting CSD related to the development of the T2S
Article 15 Obligations of the Eurosystem related to testing
Article 16 Obligations of the Contracting CSD related to testing
Article 17 Obligations of the Parties in respect of the Contracting CSDs Acceptance Tests of the T2S Services
Article 18 Obligations of the Eurosystem related to migration
Article 19 Obligations of the Contracting CSD related to migration
Article 20 Obligations of the Eurosystem related to the provision and use of the T2S Services
Article 21 Obligations of the Contracting CSD related to the provision and use of the T2S Services
Article 22 Obligations of the Parties related to the Securities Account balances
Article 23 Crisis management

CHAPTER 3  PARTICIPATION AND CONTROLLING RIGHTS OF THE CONTRACTING CSD

Article 24  Scope of the participation and controlling rights
Article 25  Change and Release Management
Article 26  Examination of T2S Services and records retention
Article 27  Governance

CHAPTER 4  INTELLECTUAL PROPERTY RIGHTS, CONFIDENTIALITY AND DATA PROTECTION

Article 28  Intellectual Property Rights
Article 29  Confidentiality
Article 30  Data protection

31 October 2011
<table>
<thead>
<tr>
<th>CHAPTER 5</th>
<th>LIABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 31</td>
<td>Standard of liability</td>
</tr>
<tr>
<td>Article 32</td>
<td>Liability rules</td>
</tr>
<tr>
<td>Article 33</td>
<td>Indemnification obligations of the Contracting CSD for acts of Third Parties</td>
</tr>
<tr>
<td>Article 34</td>
<td>Force Majeure and acts by Third Parties</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 6</th>
<th>SUSPENSION, TECHNICAL DISCONNECTION, DURATION AND TERMINATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 35</td>
<td>Right of suspension by the Eurosystem</td>
</tr>
<tr>
<td>Article 36</td>
<td>Right of technical disconnection by the Eurosystem</td>
</tr>
<tr>
<td>Article 37</td>
<td>Term</td>
</tr>
<tr>
<td>Article 38</td>
<td>Termination for cause</td>
</tr>
<tr>
<td>Article 39</td>
<td>Termination for convenience</td>
</tr>
<tr>
<td>Article 40</td>
<td>Financial consequences of termination</td>
</tr>
<tr>
<td>Article 41</td>
<td>Duties of the Parties after notification of termination</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHAPTER 7</th>
<th>MISCELLANEOUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 42</td>
<td>Dispute resolution and escalation</td>
</tr>
<tr>
<td>Article 43</td>
<td>Arbitration</td>
</tr>
<tr>
<td>Article 44</td>
<td>Own fees and costs</td>
</tr>
<tr>
<td>Article 45</td>
<td>Public announcements</td>
</tr>
<tr>
<td>Article 46</td>
<td>Entire Agreement and non-retroactivity</td>
</tr>
<tr>
<td>Article 47</td>
<td>Amendments</td>
</tr>
<tr>
<td>Article 48</td>
<td>No waiver</td>
</tr>
<tr>
<td>Article 49</td>
<td>Survival</td>
</tr>
<tr>
<td>Article 50</td>
<td>Notices</td>
</tr>
<tr>
<td>Article 51</td>
<td>Invalid or incomplete provisions</td>
</tr>
<tr>
<td>Article 52</td>
<td>No agency or transfer of undertaking</td>
</tr>
<tr>
<td>Article 53</td>
<td>Joint liability</td>
</tr>
<tr>
<td>Article 54</td>
<td>Choice of law</td>
</tr>
</tbody>
</table>
## LIST OF SCHEDULES

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule 1</td>
<td>Definitions</td>
</tr>
<tr>
<td>Schedule 2</td>
<td>T2S Programme Planning and Monitoring</td>
</tr>
<tr>
<td>Schedule 3</td>
<td>User Testing</td>
</tr>
<tr>
<td>Schedule 4</td>
<td>Migration</td>
</tr>
<tr>
<td>Schedule 5</td>
<td>T2S Service Description</td>
</tr>
<tr>
<td>Schedule 6</td>
<td>T2S Service Level Agreement</td>
</tr>
<tr>
<td>Schedule 7</td>
<td>Pricing</td>
</tr>
<tr>
<td>Schedule 8</td>
<td>Governance</td>
</tr>
<tr>
<td>Schedule 9</td>
<td>Change and Release Management</td>
</tr>
<tr>
<td>Schedule 10</td>
<td>Information Security</td>
</tr>
<tr>
<td>Schedule 11</td>
<td>Exit Management</td>
</tr>
<tr>
<td>Schedule 12</td>
<td>Form for Subcontracting</td>
</tr>
<tr>
<td>Schedule 13</td>
<td>Procedure for payment of claims</td>
</tr>
</tbody>
</table>
T2S Framework Agreement

This Agreement is entered into on the Agreement Date between [• insert name and place of registered office of acting euro area NCB/ECB] acting in the name and on behalf of all of the members of the Eurosystem

and

[• insert name and place of registered office of Contracting CSD] (hereinafter the ‘Contracting CSD’)

The parties to this Agreement are referred to collectively as the ‘Parties’ or individually as a ‘Party’.

PREAMBLE

(1) On 17 July 2008, the Governing Council decided to launch the T2S Programme aimed at setting up a service to support securities settlement in Central Bank Money, to be provided to Central Securities Depositories (CSDs) under the name ofTARGET2-Securities (T2S). As part of the Eurosystem’s tasks in accordance with Articles 17, 18 and 22 of the Statute of the European System of Central Banks and of the European Central Bank (hereinafter the ‘Statute of the ESCB’), T2S aims to facilitate post-trading integration by supporting core, neutral and borderless pan-European cash and securities settlement in Central Bank Money so that CSDs can provide their customers with harmonised and commoditised settlement services in an integrated technical environment with cross-border capabilities. The Governing Council also entrusted the 4CB with developing and operating T2S, as part of an internal distribution of work within the Eurosystem.

(2) On 16 July 2009, the Eurosystem and the Contracting CSD as well as other CSDs, entered into the T2S Memorandum of Understanding showing their support for the T2S Programme upon the terms set out therein and setting certain mutual obligations and responsibilities for the time period up to the conclusion of a definitive agreement.

(3) On 21 April 2010 the Governing Council adopted Guideline ECB/2010/2 of 21 April 2010 on TARGET2-Securities¹, which lays down the basic foundations of the T2S Programme in its Development Phase and further specifies the Eurosystem’s governance procedures applicable in this context.

(4) The Contracting CSD, which is a CSD regulated and authorised under specific laws and regulations to act, inter alia, as an operator of Securities Settlement Systems, will use the T2S Services for securities settlement in Central Bank Money. The Contracting CSD will outsource certain IT development and operational activity to the Eurosystem, as necessary for the Eurosystem to operate T2S. The Contracting CSD will maintain full control over the business and contractual relationship with its customers and over the parameters of its business operations, which includes the Contracting CSD’s ability to monitor and control the processing of its business operations in T2S in accordance with the terms of this Agreement. T2S is a settlement solution and is not a CSD nor a Securities Settlement System.

(5) In view of the above, this Agreement sets out the rights and obligations of the Parties.
CHAPTER 1
SCOPE, DEFINITIONS AND CONSTRUCTION

Article 1
Scope

1 This Agreement sets out the rules that govern, inter alia:

   (a) the cooperation in the Development Phase of T2S, during which the Eurosystem will develop the T2S Services in accordance with Schedule 2 (T2S Programme Planning and Monitoring), the T2S Scope Defining Set of Documents, and Schedule 5 (T2S Service Description); and

   (b) the provision of the T2S Services by the Eurosystem to the Contracting CSD in the Operational Phase, and the Contracting CSD’s use of the same, as specified in Schedule 5 (T2S Service Description).

2 The purpose of the Development Phase is to establish the T2S Services to be provided by the Eurosystem in the Operational Phase.

3 The Contracting CSD shall have no contractual relationship with the 4CB, other than in the capacity of each of these four Central Banks as members of the Eurosystem, and waives any recourse against the 4CB in connection with the matters covered by this Agreement to the extent permissible by applicable law.

4 The Eurosystem shall have no contractual relationship with the Contracting CSD’s customers related to the Eurosystem’s provision of T2S Services to the Contracting CSD. The Contracting CSD shall remain exclusively responsible for its business and contractual relations with its customers, including Directly Connected Parties (DCPs), in relation to its services enabled by the Eurosystem’s provision of the T2S Services, or other services provided in the Contracting CSD’s capacity as a CSD or as an operator of a Securities Settlement System.

5 The Contracting CSD shall remain exclusively responsible for its relationship with the Relevant Competent Authorities regarding its use of the T2S Services. Without prejudice to other provisions of this Agreement, the Eurosystem shall refrain from intervening in this relationship without the Contracting CSD’s prior written consent or request. The rights and obligations of the Parties in this respect are further detailed in Article 8.

6 This Agreement sets out the scope of the T2S Services.

1 OJ L 118, 12.5.2010, p. 65.
Article 2

Definitions and construction

1 In this Agreement references:

(a) to applicable laws, Schedules, Annexes or other documents shall be deemed to refer, unless specified otherwise, to the respective applicable laws, Schedules, Annexes or other documents;

(b) to this Agreement (whether included in the Articles of the Agreement or in a Schedule or an Annex) shall include the Schedules and the Annexes;

(c) to ‘include’, ‘includes’, ‘including’, ‘in particular’ or ‘e.g.’ means ‘without limitation’;

(d) to persons shall include individuals (natürliche Personen) and legal entities (juristische Personen) and shall include the permitted transferees and assignees of such individuals and legal entities;

(e) to the holder of any office or position of responsibility include references to such person as is from time to time appointed to exercise the functions of the holder;

(f) to any service or other matter or item as described, listed or specified in this Agreement shall include references to such service or other matter or item as removed, replaced, amended or edited from time to time under the terms of this Agreement; and

(g) words in the plural shall have the same meaning when used in the singular and vice versa.

2 The heading and table of contents of this Agreement shall not affect its construction or interpretation.

3 This Agreement is composed of the Preamble and of Articles 1 to 54 as well as of Schedules 1 to 13 and the Annexes to the Schedules. The Schedules and the Annexes to the Schedules form part of this Agreement and shall have the same force and effect as if expressly set out in Articles 1 to 54. Schedule 1 (Definitions) sets out the meaning of the terms in this Agreement, which are written with initial capital letters, other than proper nouns or titles of the Schedules to the Agreement. In the event of a conflict between stipulations contained in Articles 1 to 54 and those contained in a Schedule or an Annex, as the case may be, the stipulations contained in Articles 1 to 54 shall prevail. In the event of a conflict or inconsistency between Schedule 1 (Definitions) and the other Schedules, or between such other Schedules, Schedule 1 (Definitions) shall prevail over the other Schedules and shall be used to resolve conflicts or inconsistencies between such other Schedules. In the event of a conflict between a Schedule and an Annex, the terms of the Schedule shall prevail. In the event of a conflict or inconsistency between this Agreement and any other document referenced or referred to in it, this Agreement shall prevail.
Where this Agreement contains a German term as a translation of an English term, the German term shall be binding for the interpretation of this Agreement.

The T2S Scope Defining Set of Documents shall be part of this Agreement, unless and to the extent expressly specified to the contrary in this Agreement or in the T2S Scope Defining Set of Documents. In case of such specification, the relevant part of the T2S Scope Defining Set of Documents shall have only interpretative value. The T2S Scope Defining Set of Documents may be complemented from time to time in accordance with Schedule 9 (Change and Release Management). The Eurosystem shall aim at ensuring consistency between the T2S Scope Defining Set of Documents and the Service Description at all times. In the event of inconsistencies between documents, the last version of the most detailed document reviewed by the Parties in accordance with Schedule 2 Annex 8 (T2S deliverables list and management process) concerning the issue shall prevail. If a requirement/function is not specified in the GFS or the UDFS, the URD shall prevail. The T2S Documentation that are not T2S Scope Defining Set of Documents are not part of this Agreement unless insofar expressly specified to the contrary in this Agreement. The T2S Documentation may be complemented from time to time by the Eurosystem in accordance with Schedule 2 Annex 8 (T2S deliverables list and management process). The Eurosystem shall make the T2S Documentation available to the Contracting CSD. The T2S Documentation is not to be understood as amending, being part of, or supplementing this Agreement unless expressly specified in this Agreement.

CHAPTER 2
RIGHTS AND OBLIGATIONS OF THE PARTIES

Article 3
Representations of the Parties

The Eurosystem represents the following at the Agreement Date and throughout the term of this Agreement:

(a) in accordance with Articles 17, 18 and 22 of the Statute of the ESCB, the Eurosystem has and shall maintain in effect all the necessary statutory powers and authorisations to provide the T2S Services in performance of its public tasks;

(b) the execution and performance of this Agreement have been duly authorised by all necessary action of the decision-making bodies of the Eurosystem, in accordance with the Statute of the ESCB.

The Contracting CSD represents the following:

(a) at the Agreement Date and throughout the term of this Agreement that the execution and performance of this Agreement have been duly authorised by all necessary action of the decision-making or other relevant bodies of the Contracting CSD.
as from the Migration Date and as from then throughout the term of this Agreement and without prejudice to Article 38(3)(a), the Contracting CSD has and shall maintain in effect all the necessary rights, powers, and authorisations to perform its obligations under this Agreement, including, in particular, all licenses, permits and consents required in order to use the T2S Services.

**Article 4**

**Multilateral Character of T2S**

1 The Parties acknowledge that T2S is multilateral in character in that it aims at facilitating European post-trading integration by supporting cash and securities settlement in Central Bank Money, thereby combining the interests of Participating CSDs, Central Banks and all other T2S Actors. The Parties agree that actions that would have a material negative impact on any of the CSDs participating in T2S or would not be in line with the aim of achieving securities settlement in Central Bank Money are incompatible with the Multilateral Character of T2S. The T2S Services shall be provided to CSDs participating in T2S on the basis of uniform requirements and Governance rules, which include a framework for Specific Changes. The Contracting CSD acknowledges that the Eurosystem will offer Parallel Framework Agreements to all CSDs that are eligible to use the T2S Services in accordance with the conditions set out in Article 5.

2 The Parties shall use reasonable efforts to cooperate with each other in identifying any subject matters related to T2S that would benefit from further harmonisation and in supporting consequent adaptations to the legal and regulatory framework. The Contracting CSD shall use reasonable efforts to adapt its operational, internal guidelines as well as its processes and related technical systems in order to foster the development of the European post-trading infrastructure, make efficient use of the T2S Services and maintain the Multilateral Character of T2S. The Eurosystem shall use reasonable efforts to adapt its operational, internal guidelines as well as its processes and related technical systems in order to foster the development of the European post-trading infrastructure and maintain the Multilateral Character of T2S.

**Article 5**

**Non-discriminatory access**

1 The Eurosystem may allow any CSD to access the T2S Services if it is eligible in accordance with the Access Criteria, as specified in the paragraph 2. The Eurosystem shall apply such Access Criteria in a fair and non-discriminatory manner.

2 CSDs shall be eligible to access T2S Services as Participating CSDs provided they:

(a) have been notified to the European Securities and Markets Authority (ESMA) under Article 10 of Directive 98/26/EC or, in the case of a CSD from a non-European
Economic Area jurisdiction, operate under a legal and regulatory framework that is equivalent to that in force in the Union Member States;

(b) have been positively assessed by the Relevant Competent Authorities against the CESR/ESCB Recommendations for Securities Settlement Systems;

(c) make each security/International Securities Identification Number (ISIN) for which they are an Issuer CSD (or Technical Issuer CSD) available to other Participating CSDs upon request;

(d) commit to offer to other Participating CSDs Basic Custody Services on a non-discriminatory basis;

(e) commit to other Participating CSDs to carry out their settlement in Central Bank Money in T2S if the relevant currency is available in T2S.

3. The Contracting CSD shall comply with the Access Criteria at the latest from the date of its migration to T2S and throughout the term of this Agreement. The Eurosystem shall assess the compliance with the Access Criteria. The Contracting CSD shall promptly inform the Eurosystem of any change affecting its compliance with the Access Criteria occurring during the term of this Agreement. If deemed appropriate, the Eurosystem may reassess the compliance with the Access Criteria. The Contracting CSD agrees that the Eurosystem has the right to request at any time confirmation and evidence regarding its compliance with the Access Criteria.

4. The Eurosystem may grant a derogation from the Access Criterion set out in paragraph 2(e) in line with Decision (ECB/2011/XX).

Article 6

Duty of loyal cooperation and information

In the exercise of its rights and the performance of its obligations under this Agreement each Party shall:

(a) act in good faith and collaborate with the other Party closely and transparently in their contractual relations; and

(b) promptly give to the other Party notice of facts and any information that may reasonably affect its own or the other Party’s ability to perform its obligations under this Agreement in any material respect.
Article 7
Assignment and subcontracting

1. The Contracting CSD shall inform the Eurosystem as soon as reasonably practicable if it has outsourced or subcontracted any part of its obligations under this Agreement to a Third Party. Where the Contracting CSD outsources or subcontracts any of its tasks, it shall remain liable to the Eurosystem for the performance of its duties and obligations under this Agreement.

2. Any assignment or transfer of a right or an obligation of a Party arising out of or in connection with this Agreement shall be subject to the prior written approval of the other Party and such approval may not be unreasonably withheld or delayed. Such approval shall not be required for (a) the assignment or transfer of a right to an Affiliate of a Party; or (b) the assignment or transfer of a right enabling the exercise of a right of recourse of an insurance company of a Party to the extent that the claim or damage suffered by that Party is subrogated to such insurance company.

3. Due to the public nature of T2S, the operation and running of T2S can only be entrusted to one or more euro area national central banks (NCBs). The development and operation of T2S is performed by the 4CB, by an Affiliate of the 4CB, or by one or more euro area NCBs belonging to the 4CB, as part of an internal distribution of work within the Eurosystem and is not to be considered as assigning, transferring, outsourcing or subcontracting within the meaning of this Article. The Eurosystem may outsource or subcontract to a Third Party its tasks under this Agreement that are material for the performance of the Eurosystem’s obligations under this Agreement only with the express, prior and written consent of the CSD Steering Group (CSG) as described in paragraph 4 and such approval may not be unreasonably withheld or delayed. Outsourcing and subcontracting within the meaning of this Article do not include the procurement of services which are not core tasks that CSDs outsource to the Eurosystem, and therefore no consent of the CSG is needed for such outsourcing and subcontracting. The dispute resolution mechanism set up in Article 42 shall apply in case of disagreement.

4. Where the consent of the CSG referred to in paragraph 3 is needed, the Eurosystem shall pre-advise the CSG, the Contracting CSD and each Participating CSD as soon as possible of any planned action, and shall give reasonable prior notice with details of the proposed terms and conditions pursuant to which such action would take place and shall request the consent of the CSG. The CSG shall give its response within 14 calendar days by providing its consent or reasoned refusal of consent or by indicating within which deadline it would be able to provide an answer to the Eurosystem. In any event, such additional time to respond shall not exceed four weeks from the receipt of the request. The CSG shall approve its consent by a double majority vote of the CSDs as set out in Schedule 8 (Governance). The consent shall be deemed to be given to the Eurosystem if it has been provided by a double majority of the CSDs that responded to the Eurosystem request within 14 calendar days from receiving the Eurosystem’s request or, if applicable, within the additional time to respond as described above. Where a reply from a CSD or the CSG does not reach the Eurosystem within 14 calendar days or, if applicable, within the additional time to respond as described above, this is considered implied consent to the outsourcing or subcontracting.
5. Where the Eurosystem outsources or subcontracts any of its tasks in accordance with paragraph 3, it shall remain liable to the Contracting CSD for the performance of its duties and obligations under this Agreement. If the Eurosystem outsources or subcontracts a task to a Third Party, it shall ensure, as much as appropriate, that its subcontractors are bound by confidentiality and data protection obligations. If the task outsourced or subcontracted by the Eurosystem is a material task, it shall also ensure that its subcontractors are subject to Business Continuity and Disaster Recovery arrangements similar to those contained in this Agreement and that it retains an adequate level of control over such Third Party, including, if necessary, a right to access the subcontractor’s relevant premises, records, systems and/or staff. The Eurosystem, in defining its subcontractors’ obligations, shall take into account the need to ensure adequate cooperation with the Contracting CSD for the purpose of helping the Contracting CSD as a regulated entity to meet its Legal and Regulatory Requirements.

6. The Parties shall in addition use the form contained in Schedule 12 (Form for Subcontracting) in connection with the obtaining and granting of consent to subcontract.

Article 8

Compliance with Legal and Regulatory Requirements, separation of functions

1. Both Parties acknowledge that this Agreement is without prejudice to the Legal and Regulatory Requirements applicable to the Contracting CSD concerning inter alia the powers and responsibilities of the Relevant Competent Authority and consequently shall have no influence on such powers and responsibilities, which remain exclusively in charge of the supervision and oversight of the Contracting CSD. As regards access to relevant information and on-site inspections, the Relevant Competent Authorities maintain the legal and regulatory powers applicable under the jurisdiction in which the CSD operates.

2. Both Parties recognise that the Contracting CSD is directly responsible to the Relevant Competent Authorities with regard to compliance with the Legal and Regulatory Requirements and that in neither of these functions have the Contracting CSD’s responsibilities been delegated to the Eurosystem. The Contracting CSD shall exercise its rights and perform its obligations under this Agreement at all times in compliance with the applicable Legal and Regulatory Requirements and shall ensure that its staff, agents and employees act in compliance with such requirements. The Contracting CSD shall promptly inform the Eurosystem of all Legal and Regulatory Requirements applicable to it and any changes to such requirements or any evolutions in their interpretation and application, when compliance with such requirements needs to be considered in connection with the provision or use of the T2S Services. The Eurosystem shall provide reasonable assistance to the Contracting CSD in meeting its Legal and Regulatory Requirements and in ensuring that the Contracting CSD’s use of the T2S Services does not lead to non-compliance with such requirements, to the extent that it was informed by the Contracting CSD and to the extent that such requirements are compatible with the Multilateral Character of T2S.

3. The Eurosystem shall maintain contact with the relevant Union institutions and bodies, and the Relevant Competent Authorities to the extent necessary under this Agreement.
4. Each of the Eurosystem Central Banks shall maintain at all times a clear separation be-
tween (a) its role as a Party to this Agreement; (b) its regulatory, supervisory and oversight 
functions; and (c) its function as an operator of its own CSD, if applicable.

5. Based on Articles 127 of the Treaty on the Functioning of the European Union and Article 
3 of the Statute of the ESCB, in the T2S context, the Eurosystem shall in particular:

   (a) exclusively exercise full control over all cash accounts in euro in T2S, i.e. operate the 
cash accounts it holds for its banks and safeguard the integrity of the euro which, for 
the purposes of this Agreement, includes the implementation of monetary policy in-
cluding all central bank credit operations as well as settlement in Central Bank Mo-
ney in the euro;

   (b) contribute to the smooth conduct of policies pursued by the Relevant Competent Au-
thorities relating to the prudential supervision of credit institutions and the stability 
of the financial system;

   (c) ensure that it does not distort a level playing field for market participants;

   (d) carry out efficient oversight of their market infrastructure while preserving the sepa-
ration of this function in line with paragraph 4 above.

6. To the extent relevant and subject to the Currency Participation Agreements, non-euro area 
NCBs shall have the same rights in T2S as the Eurosystem in relation to their respective 
currencies.

7. The Eurosystem shall promote good governance aimed at avoiding conflicts between the 
non-euro NCBs operating and oversight functions.

---

**Article 9**

**Availability of expert personnel**

Each Party shall ensure that sufficient and qualified personnel, who have appropriate expertise 
and are trained in the tasks in which they are engaged, are used to perform the duties and obliga-
tions under this Agreement.

---

**Article 10**

**Compliance with Information Security requirements**

1. The Eurosystem shall in accordance with and as described in Schedule 10 (Information 
Security):

   (a) implement the Information Security framework for T2S;

   (b) implement a process to manage Information Security in T2S by: (i) regularly re-
viewing the implementation, and (ii) regularly updating the T2S Security Require-
ments to keep them in line with technical developments;
(c) maintain the T2S Threat Catalogue;

(d) perform all activities related to Information Security in accordance with the provisions set out in Schedule 10 (Information Security);

(e) report the results of Information Security reviews to the Contracting CSD;

(f) report Information Security incidents to the Contracting CSD in accordance with the provisions set out in Schedule 10 (Information Security);

(g) provide all other relevant information to the Contracting CSD to allow it to fulfil its own risk management obligations.

2. In view of ensuring Information Security for T2S, the Contracting CSD shall:

(a) ensure its own compliance with Information Security requirements according to its internal standards, Legal and Regulatory Requirements and/or best practices;

(b) report Information Security incidents to the Eurosystem, if T2S or other T2S Actors might be impacted by such incidents;

(c) report to the Eurosystem newly identified threats or detected gaps that might threaten T2S Information Security.

3. The parties shall cooperate according to the following provisions:

(a) The Eurosystem shall at least on a yearly basis deliver for review to the Contracting CSD the T2S Information Security Risk Evaluation Table and the T2S Information Security Risk Treatment Plan, as further specified in section 4.2 of Schedule 10 (Information Security);

(b) The Eurosystem shall maintain a consolidated action plan for all risks appearing in a T2S Information Security Risk Treatment plan, which require follow-up, and shall deliver for review to the Contracting CSD an updated version of the action plan at least on an annual basis, as further specified in section 4.2.2 of Schedule 10 (Information Security);

(c) The Eurosystem shall set up a multilateral coordination substructure, in accordance with the Governance, for the coordination and monitoring of the T2S Information Security Risk Management activities, as further specified in section 4.3 of Schedule 10 (Information Security);

(d) If a disagreement arises in the substructure, each Party shall be entitled to escalate the issue to the Steering Level and shall have, if the disagreement persists, the ultimate possibility to initiate the dispute resolution procedure specified in Article 42, as further specified in section 4.3 of Schedule 10 (Information Security);

(e) If a new Information Security risk is identified, or if an existing Information Security risk obtains a higher likelihood or impact score, the Eurosystem shall communi-
cate such changes to the Contracting CSD in accordance with the incident response times specified in Schedule 6 (Service Level Agreement), as further specified in section 4.3 of Schedule 10 (Information Security);

4. Any matters related to operational risk, which are not covered by this Article or in Schedule 10 (Information Security), will be managed directly by the Steering Level.

5. The Eurosystem will implement an appropriate risk management framework and inform the CSDs monthly about the risk situation.

Article 11
T2S Network Service Provider

1. The Eurosystem shall allow the Contracting CSD and its DCPs to connect its IT systems to the T2S Platform, either via a Value-added Connection or via a Dedicated Link Connection.

2. The Contracting CSD shall inform the Eurosystem about the solution it has chosen for its connection to T2S at least six months prior to the intended start date of its testing activities.

3. The Contracting CSD shall use reasonable efforts to ensure that its own connectivity with the T2S Platform functions properly at all times. The Contracting CSD shall provide in its rules or contractual terms for an obligation to be imposed on its DCPs to use reasonable efforts to ensure that their connectivity with the T2S Platform functions properly at all times.

4. The Contracting CSD shall inform the Eurosystem of its intention to change its Network Service Provider (NSP) as soon as reasonably possible.

5. As far as the Value-added Connections are concerned, the following provisions shall apply:

(a) The Eurosystem shall communicate to the Contracting CSD during the Development Phase in accordance with Schedule 2 the NSPs that it has selected for the provision of Connectivity Services to the Contracting CSD. The requirements according to which the NSPs have been selected, and which they need to comply with, are specified in the attachments 1 (technical requirements) and 2 (business requirements) of the Licence Agreement, which has been and will be kept public on the website of the Banca d’Italia. Changes to these requirements will be managed in accordance with Schedule 9 (Change and Release Management) and the Licence Agreement.

(b) The Eurosystem shall exercise due care in the coordination of the Contracting CSD’s monitoring of the compliance of the NSP(s) with those requirements pursuant to paragraph 5(a) which the Contracting CSD can monitor itself. The Eurosystem shall exercise due care in the monitoring of the compliance of the NSP(s) with those requirements which the Contracting CSD cannot monitor itself. The Eurosystem shall address material breaches of such requirements in accordance with the relevant con-
T2S Framework Agreement

tractual provisions with the NSP(s). If the Contracting CSD connects to T2S via an NSP in respect of which the Eurosystem has identified a material breach or a potential material breach of the requirements, the Eurosystem will inform the Contracting CSD about the (potential) material breach it has identified, as well as about the steps it has undertaken to remedy (or avoid) such a (potential) material breach. Should the material breach by the NSP not be remedied in a reasonable timeframe, the Eurosystem shall take the appropriate measures towards the NSP, subject to the Eurosystem’s arrangements with the NSP, and provide support to the Contracting CSD.

(c) The Contracting CSD shall carry out its own due assessment as regards the ability of the selected NSP(s) to offer a Value-added Connection to the Contracting CSD and as regards the reliability of the NSP(s) (financially, operationally, technically or otherwise) towards the Contracting CSD. The Contracting CSD may not rely solely on the results of the selection process undertaken by the Eurosystem regarding the selection of the NSP(s).

(d) The Eurosystem shall not be responsible for any cost or loss that the Contracting CSD may incur as a result of a need to transition to a different NSP if the NSP with which the Contracting CSD has contracted the Connectivity Services loses, for whatever reason, its status as an NSP.

(c) For the avoidance of doubt, the Contracting CSD and the DCP shall not be responsible to the Eurosystem for the acts and omissions of its NSP(s). The Contracting CSD shall inform the Eurosystem about any concerns it may have regarding the operational, technical or financial reliability of its NSP(s) as well as any performance issues regarding delivery of the Value-Added Connection provided by its NSP(s). The Eurosystem shall assess whether or not the information provided by the Contracting CSD could reasonably indicate non-compliance by the NSP of the requirements referred to in paragraph 5(a). If the Eurosystem, acting reasonably, decides that the NSP does not comply with the relevant requirements, the Eurosystem shall forthwith take appropriate steps against the NSP, subject to the Eurosystem’s arrangements with the NSP. At all times, the Eurosystem shall keep the Contracting CSD informed of the steps it is taking and discuss the proposed actions with the Contracting CSD in advance.

(f) The Parties shall monitor the risk situation of the NSPs within their respective contractual relationships with their NSPs and discuss them as appropriate within the Information Security framework.

(g) The Parties shall analyse the impact on the T2S Programme Plan in accordance with Schedule 2 (T2S Programme Planning and Monitoring), whenever the Eurosystem starts a new selection process of a NSP.
(h) The provision of Connectivity Services is outside of the scope of the T2S Services and the Eurosystem is not responsible to the Contracting CSD for the acts and omissions of the NSP(s).

6. The Eurosystem shall communicate to the Contracting CSD in accordance with Schedule 2 (T2S Programme Planning and Monitoring) the entity that will offer the necessary Physical Connectivity Services for the Dedicated Link Connection, as well as the necessary specifications for the Value-added Connectivity Services, which the Contracting CSD has to implement, in order to establish a Dedicated Link Connection with the T2S Platform. The rights and obligations of the Parties related to the Dedicated Link Connection will be specified outside this Agreement.

Article 12

Directly Connected Parties

1. The Contracting CSD shall maintain a contractual relationship with the DCP that it has designated to the Eurosystem. The Eurosystem shall not maintain a contractual relationship with that DCP for the matters dealt with under this Agreement.

2. The Contracting CSD shall only have the obligations in respect of the DCP that it has designated, as provided for in this Agreement and in the T2S Scope Defining Set of Documents. The Contracting CSD shall reflect the obligations that need to be performed by the DCP in relation to the T2S Services in its contractual relationship with such DCP.

3. Without prejudice to Article 1(4), in all matters covered by the subject matter of this Agreement, and without prejudice to its provisions, the Eurosystem can interact in particular with the Contracting CSD’s DCPs for the purposes of managing the technical connections to T2S, DCP Certification in user testing and crisis management.

Article 13

Obligations of the Eurosystem related to the development of T2S

The Eurosystem shall:

(a) establish T2S in accordance with the T2S Scope Defining Set of Documents and Schedule 5 (T2S Service Description) and use reasonable efforts to allocate appropriate resources to its implementation and to respect the milestone deliverables set out in Schedule 2 (T2S Programme Planning and Monitoring) in line with the agreed procedure for modifications as defined in Schedule 2 (T2S Programme Planning and Monitoring).
T2S Framework Agreement

(b) implement Common and Specific Changes to the T2S Services as requested by the Contracting CSD and managed by the Eurosystem in accordance with Article 25 and Schedule 9 (Change and Release Management);

c) set up and maintain the T2S Programme Plan as well as assess and adjust the T2S Programme Plan with a view to ensuring effective implementation of the T2S Services;

d) report to and inform the Contracting CSD in accordance with Schedule 2 (T2S Programme Planning and Monitoring) of the progress achieved;

e) make available T2S Documentation to the Contracting CSD in line with the T2S Programme Plan;

(f) allow the Contracting CSD to review and agree the preparation of the T2S Documentation as provided for in Article 14 in line with Schedule 2 (T2S Programme Planning and Monitoring).

Article 14
Obligations of the Contracting CSD related to the development of T2S

As further specified in the relevant Schedules, the Contracting CSD shall participate and contribute to the development of T2S through the following:

(a) it shall support the Eurosystem in the preparation of the T2S Documentation in accordance with Annex 8 of Schedule 2 (T2S Programme Plan and Monitoring);

(b) it shall inform the Eurosystem whenever it has in its possession material information, be it of a technical, operational, legal, regulatory or any other nature, and that would, in the absence of any action by the Eurosystem lead to a material adverse effect to the effective and harmonised functioning of the T2S Programme and/or T2S Services;

(c) it shall use reasonable efforts to respect the milestone deliverables set out in Schedule 2 (T2S Programme Planning and Monitoring), as applicable to it, set up its own project plan for implementation of the T2S Programme, allocate resources to successive versions of the T2S Documentation, with the view to ensuring effective use of the T2S Services in accordance with the timelines referred to in Article 13(f) and report on the progress of its project plan and its readiness for the effective implementation of the T2S Services;

(d) it shall cooperate with the Eurosystem by adapting its systems and processes, especially by ensuring adequate system interfaces and reliable connections and allocate appropriate resources to the implementation of the project plan, assess and adjust such project plan, so as to allow for its operational and technical readiness for the use of the T2S Services and for the timely initiation of provision of such T2S Services;

(e) the Contracting CSD shall provide information that may be relevant for the Eurosystem to develop T2S or fulfil its tasks and responsibilities under this Agreement, including information on the settlement volumes of the Contracting CSD.
As further specified in Schedule 3 (User Testing) the Eurosystem shall:

(a) coordinate the User Testing activities and communication between the Contracting CSD and the Central Banks whose currencies are available for settlement in T2S as well as between the Contracting CSD and other CSDs participating in the User Testing activities;

(b) inform the Contracting CSD about the results of User Testing as defined in Schedule 3 (User Testing);

(c) prepare and execute the Eurosystem Acceptance Testing (EAT), and provide regular progress reporting as well as an assessment report confirming the compliance of T2S with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents before the start of User Testing;

(d) define the CSD certification tests required to assess that the Contracting CSD’s systems cannot harm T2S due to an inappropriate technical communication or operational procedure;

(e) define the DCP certification tests required to assess that the systems of the DCPs of the Contracting CSD cannot harm T2S due to an inappropriate technical communication or operational procedure;

(f) prepare the necessary non-functional tests and execute these non-functional tests in order for the Eurosystem to confirm the non-functional compliance of T2S;

(g) remedy any material deficiency defined as critical defect (priority 1) and, for any defect defined as high defect (priority 2), either directly resolve the defect or, if agreed with the Contracting CSD, as a first step, provide a technical or procedural workaround and, as a second step, resolve the defect within a specific timeframe to be defined along with the workaround to ensure that the T2S Services are established in accordance with the principles set out in Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents;

(i) provide reasonable support for testing activities of the Contracting CSD in the different stages of User Testing;

(j) cooperate with the Contracting CSD in respect of the Contracting CSD’s acceptance tests of the T2S Services in accordance with Article 17.
**Article 16**

**Obligations of the Contracting CSD related to testing**

As further specified in Schedule 3 (User Testing) the Contracting CSD shall:

(a) support the Eurosystem in the preparation of the overall User Testing calendar by providing the Eurosystem with its proposed Test Plan and User Testing calendar of its activities;

(b) execute the mandatory test cases and test scenarios for CSD certification within the period foreseen in the T2S Programme Plan for the migration wave in which it is participating;

(c) monitor that its DCPs execute the mandatory test cases and test scenarios for DCP Certification within the period foreseen in Schedule 2 (T2S Programme Planning and Monitoring) for the migration wave in which it is participating.

(d) cooperate with the Eurosystem in respect of its acceptance tests of the T2S Services in accordance with Article 17.

**Article 17**

**Obligations of the Parties in respect of the Contracting CSDs’ Acceptance Tests of the T2S Services**

1 Following the Eurosystem’s notification of its readiness to fulfil synchronisation point 8 (Start Bilateral Interoperability Testing) according to Annex 9 of Schedule 2 (T2S Programme Planning and Monitoring), the Contracting CSD shall be entitled to test the compliance of the T2S’ Services with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents in accordance with the methodology stated in this Article and in Schedule 3 (User Testing).

2 In case the Contracting CSD chooses to perform the tests as defined in paragraph 1, the Contracting CSD shall finalise such tests within 6 months following the Eurosystem’s notification of its readiness to fulfil synchronisation point 8 (Start Bilateral Interoperability Testing), unless provided otherwise in Schedule 2 (T2S Programme Planning and Monitoring). If the Contracting CSD discovers that the T2S Services do not comply with Schedule 5 (T2S Service Description) and/or the T2S Scope Defining Set of Documents, it shall follow the procedures laid down in section 5.3 of Schedule 3 (User Testing).

3 Notwithstanding the Contracting CSD’s decision to perform the tests as described in paragraphs 1 and 2, the Contracting CSD shall provide to the Eurosystem in writing, and within 6 months following the Eurosystem’s notification of its readiness to fulfil synchronisation point 8 (Start Bilateral Interoperability Testing), either that it accepts the T2S Services as compliant with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents.
T2S Framework Agreement

Documents or that it does not accept the T2S Services as compliant with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents.

4 In the case the Contracting CSD notifies the Eurosystem that it does not accept the T2S Services as compliant with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents, it shall promptly, and in no case later than within 5 working days after such notification, deliver a report to the Eurosystem describing all cases of non-compliance it has identified (Non-compliance Notification).

5 Upon the Eurosystem’s notice to the Contracting CSD that the Eurosystem has remedied individual or all cases of material non-compliance, the Contracting CSD shall test the error correction.

6 When the Contracting CSD finds that none of the reported cases of material non-compliance continues to exist, it shall provide a confirmation that it accepts the T2S Services as compliant with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents (Compliance Confirmation) in writing without undue delay.

7 The presentation of the Compliance Confirmation by the Contracting CSD to the Eurosystem shall constitute a waiver by the Contracting CSD of any right to assert any other case of material non-compliance of T2S with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents with regard to the termination right in accordance with Article 38(1)(b).

Article 18
Obligations of the Eurosystem related to Migration

As further specified in Schedule 4 (Migration) the Eurosystem shall:

(a) establish the necessary procedures and tools for Migration aimed at facilitating a smooth change-over of the Contracting CSD’s operations from its legacy systems to T2S, which shall, inter alia, support the Contracting CSD in suspending or reversing its Migration if the conditions for Migration, as defined in Schedule 4 (Migration), cannot be satisfied; and

(b) provide the Contracting CSD with support related to its activities necessary for completing the Migration.

Article 19
Obligations of the Contracting CSD related to Migration

As further specified in Schedule 4 (Migration) the Contracting CSD shall:

(a) adjust its internal systems, processes, interfaces and connections to enable its Migration to the T2S in compliance with the Access Criteria and the T2S Documentation, and to achieve operational and technical readiness for the use of the T2S Services;
T2S Framework Agreement

(b) set up its own project plan for the Migration and do whatever is reasonably required to ensure that its customers, including DCPs, are able to migrate to the T2S-enabled services of the Contracting CSD within the timeframe provided in Schedule 2 (T2S Programme Planning and Monitoring);

(c) determine, in co-operation with other Participating CSDs, the group in which it shall migrate to T2S and the date of its Migration in accordance with the criteria and the conditions, subject to the Eurosystem’s rights specified in Schedule 4 (Migration), and the time specified in Schedule 2 (T2S Programme Planning and Monitoring);

(d) migrate to T2S in accordance with the process specified in Schedule 4 (Migration) and within the timeframe provided in Schedule 2 (T2S Programme Planning and Monitoring);

(e) cooperate with the Eurosystem in documenting that its Migration has been successfully completed.

Article 20

Obligations of the Eurosystem related to the provision and use of the T2S Services

1. For the provision and use of T2S Services, the Eurosystem shall:

   (a) provide to the Contracting CSD the T2S Services specified in Schedule 5 (T2S Service Description);

   (b) implement Common and Specific Changes to the T2S Services as requested by the Contracting CSD and managed by the Eurosystem in accordance with Article 25 and Schedule 9 (Change and Release Management);

   (c) maintain the T2S Services so as to support, in cooperation with the Contracting CSD, ongoing compliance with the applicable Legal and Regulatory Requirements, as detailed in Article 8(1), without prejudice to the application of Article 25 and Schedule 9 (Change and Release Management) to changes that may need to be implemented as a result of such requirements;

   (d) reinstate operations to permit use of the T2S Services following a failure as specified in Schedule 6 (T2S Service Level Agreement);

   (e) update in a timely manner the T2S Documentation;

   (f) provide the Contracting CSD with financial statements, reports and other information on T2S on a regular basis that fairly represent the business and financial conditions, result of operations and state of the cost recovery in relation to T2S on the respective dates or for the respective periods covered by such financial statements, reports and other information.

2. Changes to the T2S Platform or T2S Business Application that need to be implemented urgently in order to restore or continue the provision of the T2S Services in accordance with the service levels specified in Schedule 6 (T2S Service Level Agreement) may be au-
tonomously decided and implemented by the Eurosystem in accordance with Schedule 6 (T2S Service Level Agreement) and the Manual of Operational Procedures (MOP). In such cases, the Eurosystem shall inform the Contracting CSD as soon as reasonably practicable on the nature and characteristics of the changes and the time in which the change shall be implemented.

3. The Eurosystem shall make available to the Contracting CSD a monthly Service Level Report to determine the degree of the Eurosystem’s compliance with Schedule 6 (T2S Service Level Agreement), in particular as regards the Key Performance Indicators (KPIs). If the Eurosystem fails to meet any of the KPIs, it shall in cooperation with the Contracting CSD:
   
   (a) investigate the underlying cause of the failure;
   
   (b) take necessary measures to minimise the impact of the failure;
   
   (c) take necessary measures to prevent the failure from recurring or report on the cause, the status and the remedies required to prevent recurrence of the failure.

Article 21
Obligations of the Contracting CSD related to the provision and use of the T2S Services

1. The Contracting CSD shall use the T2S Services once: (a) the User Testing is completed as specified in Article 16 and Schedule 3 (User Testing); and (b) Migration has been successfully completed as specified in Article 19 and Schedule 4 (Migration).

2. In pursuance of its obligation to use the T2S Services, the Contracting CSD shall, in particular:

   (a) perform the duties and responsibilities assigned to it in Schedule 6 (T2S Service Level Agreement);

   (b) support the resumption of the T2S Services following a failure as specified in Schedule 6 (T2S Service Level Agreement);

   (c) pay the fees in a timely manner and in accordance with the conditions set out in Schedule 7 (Pricing).

3. The Contracting CSD shall only present to T2S for processing Transfer Orders on behalf of customers that are ‘participants’ according to the national implementation of Article 2 of Directive 98/26/EC or, if the Contracting CSD is established outside the European Economic Area, on behalf of customers enjoying an equivalent protection to that in force for ‘participants’ pursuant to Directive 98/26/EC.

4. The Contracting CSD shall make all necessary arrangements with regard to its operational processes and contractual terms, in particular its rules, (a) to aim at harmonising definitions
of the moment of entry of Transfer Orders into the system and of the moment of irrevocability of such Transfer Orders, in accordance with Directive 98/26/EC, and (b) to ensure the unconditionality, irrevocability and enforceability of the settlement processed on the T2S Platform.

5. The Contracting CSD shall review, comment, and consent to or reject the Eurosystem report referred to in the Article 20(3). If the Contracting CSD rejects the report, and in particular the remedies proposed by the Eurosystem for preventing the recurrence of not meeting the KPIs, it may revert to the dispute resolution and escalation procedure set out in Article 42.

6. The Contracting CSD shall maintain and be responsible for the accuracy of all Securities Reference Data in T2S for which it is assigned as the Securities Maintaining Entity (SME). The Contracting CSD is the SME in T2S for all securities for which it is the Issuer CSD.

If the Contracting CSD is not the Issuer CSD for a given security, then the Contracting CSD will agree with the other Participating CSDs which Participating CSD will act as SME. The Contracting CSD agrees with the following provisions concerning the responsibilities of the SME for a given security:

(a) if the Securities Reference Data are required for settlement in T2S, the SME shall ensure that these are created in T2S in a timely manner and shall be responsible for maintaining them thereafter;

(b) if the SME is informed of or becomes aware of errors and/or omissions in the Securities Reference Data, it shall correct them within two hours;

(c) the Contracting CSD will not create Securities Reference Data for securities for which it is not the Issuer CSD or for which it has not agreed with the other Participating CSDs to act as SME.

7. The Contracting CSD, when acting as SME, acknowledges and confirms that it has obtained all authorisations, permits and licences to make available the Securities Reference Data to the Eurosystem for the purposes described in this Agreement. If legal action is commenced or threatened against the Eurosystem based on an alleged infringement of any right relating to such Securities Reference Data, the Eurosystem shall (a) notify the Contracting CSD in accordance with Article 50 as soon as reasonably practicable; (b) allow the Contracting CSD, at its expense, control of the defence of the claim (without prejudice to the Eurosystem’s right to take an active role in the proceedings at its own expense); (c) not make admissions, agree to any settlement or otherwise compromise the defence of the claim without the prior written consent of the Contracting CSD; such consent shall not be unreasonably withheld and (d) give, at the Contracting CSD’s request, reasonable assistance in connection with the conduct of the defence. If the Eurosystem should be held legally liable for the infringement of the Third Party’s right according to an Enforceable Judgement or has, with the prior written consent of the Contracting CSD, settled the claim, the Contracting CSD shall reimburse the Eurosystem in accordance with Schedule 13 (Procedures for Payment of Claims) for all payments that the Eurosystem has to make to the relevant Third Party. The consent referred to in the previous sentence shall not be unreasonably withheld. This reimbursement obligation shall not apply with regard to any
T2S Framework Agreement

Third Party claim asserted before a court outside (a) the European Union or (b) the home country of the Contracting CSD or any Participating CSD. In this case, the liability rules pursuant to Article 32 shall apply.

8. The Eurosystem may reassign the responsibility of the SME for a given security in T2S on a written request from the Contracting CSD and only if another Participating CSD accepts the responsibility as SME for this security.

9. The Eurosystem shall not reimburse the SME for any costs related to its responsibility to maintain the Securities Reference Data in T2S, nor shall it be involved in any way in any financial compensation arrangements between the Contracting CSD and the other Participating CSDs.

10. The Eurosystem shall not be liable to the Contracting CSD or the other Participating CSDs for any errors or omissions in any Securities Reference Data, nor shall it be involved in any way in the processing of any liability claims between them.

11. The Eurosystem may, upon request of the Contracting CSD and the other Participating CSDs, accept to act as SME for a given security. This shall not constitute a T2S Service and the Eurosystem shall not accept any liability in connection with its function as SME.

Article 22

Obligations of the Parties related to Securities Account balances

1. Securities Account balances of the Contracting CSD operated on the T2S Platform shall only be changed in T2S.

2. The Eurosystem acknowledges that the Transactional Data and CSD Static Data are essential to the Contracting CSD’s operations and that the Contracting CSD will rely on such Transactional Data and CSD Static Data for the operation of its Securities Accounts. The Eurosystem has no Intellectual Property Rights (IPRs) over the Transactional Data and CSD Static Data, which remain under the responsibility and control of the Contracting CSD except as provided by and/or required for the execution of this Agreement.

3. In providing the T2S Services, the Eurosystem shall process changes to Securities Account balances on the T2S Platform upon Transfer Orders through which the Contracting CSD has been instructed by its Users. The Eurosystem shall have no obligation to monitor the accuracy of the Transfer Orders and may rely in good faith on all Transfer Orders and information communicated and properly authenticated in accordance with the methods described in Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents.
4. The Eurosystem warrants that all Transactional Data and CSD Static Data shall be accessible to and available for the Contracting CSD as specified in Schedule 5 (T2S Service Description). The Contracting CSD shall report to the Eurosystem any errors as soon as reasonably practicable. The Contracting CSD shall require its DCPs to report any such errors to it as soon as reasonably practicable and it shall report such errors to the Eurosystem as soon as reasonably practicable.

5. The timing and procedures of error handling are further described in the MOP. The Parties shall collaborate and use their best endeavours to reverse any erroneous changes to any Securities Account balances.

Article 23
Crisis management

1. The Eurosystem shall manage and resolve any operational disturbances in T2S. In addition, due to the central role which T2S plays in securities settlement in connected markets, the Eurosystem shall assume a coordinating role. In particular, it shall coordinate, initiate and lead activities in connection with any event of an operational or financial nature which may impact the functioning and performance of T2S. The Eurosystem shall use its best efforts to act to protect the functioning of T2S and to operate T2S in a way that supports the financial stability of all connected markets.

2. The principles of Crisis management are laid down in the Schedule 5 (Service Description) and Schedule 6 (Service Level Agreement), whereas the procedural aspects of the Crisis management framework are set out in the MOP, without prejudice to the competence of the Relevant Competent Authorities. The Contracting CSD shall, in coordination with the Relevant Competent Authorities, use its best efforts to ensure the compatibility of its Crisis management framework with applicable laws. Moreover, the Contracting CSD shall make reasonable efforts to ensure the compatibility of its Crisis management framework with the T2S Crisis management procedures.

3. The details of the assistance to be provided by the Eurosystem in case of a Crisis are specified in the Service Level Agreement and are based on the following principles:

   (a) the Eurosystem shall have adequate organisational and personnel capacities to deal with a Crisis Situation;

   (b) the Eurosystem shall fully cooperate with the Contracting CSDs, the Participating CSDs, the Relevant Competent Authorities and ESMA in order to manage a Crisis Situation (including investigating the feasibility of and implementing reasonable workarounds);
(c) the Eurosystem shall prepare and maintain a Crisis management plan, and shall test its appropriateness together with the Contracting CSD, the Participating CSDs, the Relevant Competent Authorities and ESMA, on a regular basis;

(d) the Eurosystem shall provide a report to the Contracting CSDs, the Participating CSDs, the Relevant Competent Authorities and ESMA on the effective handling of a Crisis Situation within a reasonable period of time after such a Crisis has occurred; and

(e) the Eurosystem shall cover and where appropriate involve the DCP in the context of Crisis management.

4. The details of the assistance to be provided by the Contracting CSD in the case of a Crisis are specified in the Service Level Agreement and are based on the following principles:

(a) the Contracting CSD shall use its best efforts to fully cooperate with the Eurosystem in order to manage a Crisis Situation;

(b) the Contracting CSD shall use its best efforts to inform the Eurosystem about any potential market disturbances that may have an impact on T2S without delay;

(c) the Contracting CSD shall use its best efforts to ensure that its own Crisis management plans cover T2S Crisis scenarios;

(d) the Contracting CSD shall without undue delay inform and involve its DCP and other users about any T2S Crisis that could impact them; and

(e) the Contracting CSD shall use its best efforts to assist in the preparation and maintenance of a Crisis management plan by the Eurosystem.

5. In the case of a Crisis, the Contracting CSD shall be entitled to invoke its own Crisis management plan in full cooperation with and where relevant with the approval of the Eurosystem, the Relevant Competent Authorities and ESMA, which may include the settlement of transactions outside T2S, unless this would have a detrimental impact on financial stability.

---

CHAPTER 3
PARTICIPATION AND CONTROLLING RIGHTS
OF THE CONTRACTING CSD

Article 24
Scope of the participation and controlling rights

1. The participation and controlling rights of the Contracting CSD during the Development Phase shall include the following:
T2S Framework Agreement

(a) the right to submit Change Requests in accordance with the Change and Release Management procedure described in Article 25 and Schedule 9 (Change and Release Management);

(b) the right to be represented and to participate in the Governance, as specified in Article 27 and Schedule 8 (Governance);

(c) the right to obtain information as otherwise provided for in this Agreement.

2. The participation and controlling rights of the Contracting CSD during the Operational Phase shall include the following:

(a) the right to submit Change Requests in accordance with the Change and Release Management procedure set out in Article 25 and Schedule 9 (Change and Release Management);

(b) technical and operational examinations by the External Examiner in line with the multi-year T2S examination plan and the Contracting CSD’s right to request special examinations by the External Examiner, in accordance with Article 26(1) to (5) of this Agreement;

(c) the right to be represented and to participate in the Governance as specified in Article 27 and Schedule 8 (Governance);

(d) the right to obtain information as otherwise provided for in this Agreement.

3. The rights set out in paragraphs 1 and 2 shall be exercised without prejudice to Article 8 and the principle of Central Bank independence set out in Article 130 and Article 282(3) of the Treaty on the Functioning of the European Union, Article 7 of the Statute of the ESCB and in relevant national legislation.

Article 25

Change and Release Management

1. The Parties may propose Change Requests for the T2S Business Application, the T2S Scope Defining Set of Documents and requirements for NSPs. Such proposal shall be made and dealt with in accordance with Schedule 9 (Change and Release Management).

2. Change and Release Management shall adhere to the following principles:

(a) T2S is aimed at accommodating market evolution and supporting innovation;

(b) without prejudice to the right of the Contracting CSD to submit a request for the implementation of Specific Changes, new or changed services within T2S shall be provided with the objective of being available to all CSDs and Central Banks in T2S, and through them to T2S Users;

(c) without prejudice to the ultimate decision-making powers of the Governing Council, as set out in Schedule 8, no individual Participating CSD shall have a veto right with
(d) T2S shall endeavour to facilitate the Contracting CSD’s and the other Participating CSDs’ compliance with their respective Legal and Regulatory Requirements, to the extent that the Eurosystem was informed by the Contracting CSD and the other Participating CSDs about such requirements and to the extent that they are compatible with the Multilateral Character of T2S;

(e) it is the Contracting CSD’s (or respectively, another Participating CSD’s) responsibility to involve their respective user communities throughout the whole Change and Release Management;

(f) the Eurosystem shall continue to be committed to communicating information in a transparent manner towards the market in line with Schedules 8 (Governance) and 9 (Change and Release Management);

(g) the development of specific functionalities to accommodate national specificities shall be limited as much as possible. Instead, where applicable, building the necessary interfaces to let the Contracting CSD, Participating CSDs and Central Banks offer these national specificities on their platforms, with no impact on T2S, shall be favoured.

(h) in the case of changes in respect of Legal and Regulatory Requirements which apply only to one, or a few CSDs or Central Banks, Specific Changes will be available in accordance with paragraph 3 below;

(i) sufficient time shall be allotted to implement any changes needed for the Eurosystem to develop the T2S Services on a consistent basis and provide enough lead time for the Contracting CSD or another Participating CSD to change their own internal systems, processes, interfaces and connections accordingly.

3. The following principles apply to Specific Changes:

(a) the Contracting CSD, a Participating CSD or a Central Bank which has a specific need, triggered by Legal and Regulatory Requirements or by innovation/improvements, may request a new functionality, provided that this does not endanger the Lean Scope of T2S and is not incompatible with the Multilateral Character of T2S; and

(b) the requesting CSD or Central Bank shall formally commit itself to bear the financial consequences of the Specific Change in accordance with Schedule 7 (Pricing); and/or

(c) the associated costs shall be shared among all CSDs and/or Central Banks making use of the given functionality in accordance with Schedule 7 (Pricing); and

(d) the Specific Changes shall be approved in accordance with Schedule 9 (Change and Release Management); and

(e) no Specific Changes may be implemented if this imposes changes to existing features, functionalities, processes or interfaces or a deterioration of the service level of other CSDs or Central Banks, that have not approved such Specific Changes and unless these CSDs or Central Banks agree to them.
4. In accordance with Article 28(2) but subject to Article 28(3), the Contracting CSD waives any IPRs that it may have acquired in connection with the proposed changes to the T2S Services or that may have arisen in the context of Change and Release Management. Should any other legal entity or natural person who would have been associated directly or indirectly with the Change and Release Management Procedure, have acquired IPRs in connection with the proposed changes, the Contracting CSD shall: (a) inform the Eurosystem as soon as it becomes aware of potential IPRs vested in such a legal entity or natural person; and (b) use its best endeavours to ensure that such legal entity or natural person also waives any IPRs acquired in the abovementioned context.

5. In the case of refusal to implement changes triggered by Legal and Regulatory Requirements, the Governing Council shall provide a full written explanation of the reasons for the refusal.

6. The full financial consequences related to Common Changes and Specific Changes shall be recovered in accordance with Schedule 7 (Pricing).

7. Authorised changes and defect resolutions the implementation of which is pending are prioritised based on a scoring mechanism. The definition of the release is based on this priority rating taking into account the business and legal criticality of changes, the associated risks, budgetary implications and the capacity for Common Changes and Specific Changes. The approval of the content of the release and the final prioritisation are carried out as described in Schedule 8 (Governance).

Article 26

Examination of T2S Services and records retention

1. Without prejudice to the principle of Central Bank independence in performance of its public tasks, as established under Article 130 and Article 282(3) of the Treaty on the Functioning of the European Union and in the relevant national legislation, the performance of T2S Services shall be subject to technical and operational examinations performed by the External Examiner appointed by the Governing Council on the proposal of the CSG and after consultation with the Non-euro Currencies Steering Group. The costs of the External Examiner, both for regular examinations and for the special examinations according to paragraphs 4 and 6, shall be shared in equal parts between the Eurosystem, on the one side, and the Contracting CSD and the Participating CSDs, on the other.

2. The External Examiner shall be a well-reputed, internationally active accounting firm. It shall perform its services within the scope set by the Governing Council and in accordance with internationally recognised audit standards such as the Statement on Standards for Attestation Engagement (SSAE) No 16 or International Standards for Assurance Engagements (ISAE) No. 3402. The External Examiner shall be changed every 4 years.

3. The Governing Council shall set the External Examiner’s mission statement and a multi-year examination plan, taking into account examination items proposed by the CSG. The scope of the regular examinations or special examinations should be limited to the provision of T2S Services or directly related activities. The objective of these examinations is to
gives to the CSG reasonable assurance about whether (a) the organisation set up by the Eurosystem meets the obligations established in this Agreement and (b) the controls implemented by the Eurosystem are suitably designed to meet the security objectives. Moreover, the External Examiner shall deliver an opinion on the effectiveness of the controls performed by the Eurosystem on the basis of the results of the compliance check reviews and of the risks assessment and related treatment plans managed by the Eurosystem. The CSG may also propose to the Governing Council to approve any special examinations to be conducted by the External Examiner outside the multi-year examination plan.

4. Where a special examination is necessary because of a severe incident or a material and ongoing problem which has disrupted the proper functioning of the T2S Platform or the provision of T2S Services, the External Examiner shall have access to the relevant technical documentation.

5. Following the submission of the External Examiner’s report of its regular examination, the CSG shall hold an annual meeting, or, in case of a special examination, an extraordinary meeting, with the External Examiner to review the submitted report and to discuss solutions for the identified issues. The report and recommended solutions for the identified issues shall then be submitted to the Governing Council. Within 3 months of receiving the report, the Governing Council shall reply whether it accepts or rejects each of the recommended solutions. If it accepts a recommendation, the Governing Council will describe how it intends to implement such recommendation and in what timeframe. The External Examiner shall then monitor the Eurosystem’s progress on implementing the accepted recommendations and report back to the CSG at the annual meeting. If a recommendation is rejected, the Governing Council shall communicate the reasons to the CSG and the Relevant Competent Authority.

6. Without prejudice to paragraph 3, the Contracting CSD shall have the right to: (a) propose to the CSG items for the regular examinations and requests for special examinations to be conducted by the External Examiner; (b) receive all External Examiner reports; and (c) request the External Examiner to provide additional explanations to the CSG during an annual meeting referred to in paragraph 5 or in written form following such annual meeting and within its remit. The Contracting CSD and/or the Relevant Competent Authorities shall have the right to propose special examinations to be conducted by the External Examiner directly to the Governing Council.

7. If the Governing Council refuses to appoint the External Examiner proposed by the CSG as provided for in paragraph 1 or to include items for the regular or special examination to be conducted by the External Examiner upon the CSG’s proposal, the Governing Council shall communicate the reasons for its refusal to the CSG, to the Contracting CSD and/or to the Relevant Competent Authorities. The CSG, the Contracting CSD and/or the Relevant Competent Authorities may submit new proposals to the Governing Council until a mutually agreeable solution is found.

8. The Eurosystem shall ensure that the External Examiner has the following rights and obligations related to the performance of its examinations and checks:

   (a) the External Examiner shall contact the Eurosystem through the indicated contact persons. The External Examiner shall give the Eurosystem prior notice of 14 calendar days before starting the regular examination or an additional check and shall inform the Eurosystem of the following: (a) the object of the examination or check; (b)
the names of the authorised representatives of the External Examiner who shall carry out the examination or check; (c) the Eurosystem offices at which the examination or check is to be conducted; (d) the methods to be applied; and (e) the time schedule;

(b) the External Examiner shall have the right to examine technical and operational documentation and records, whether in written or electronic form, directly relevant for assessing the performance of the T2S Services and for the setting of the T2S pricing policy and the implementation of the T2S Programme budget. Such technical and operational documentation and records shall be made available, upon request, to the External Examiner’s authorised representatives during normal business hours at the relevant Eurosystem offices. The External Examiner shall have the right to make, for its own internal use only, copies and excerpts from the documentation and records made available by the Eurosystem. Such copies and excerpts shall be listed in a transmission protocol and returned to the Eurosystem upon completion of the examination or check and upon confirmation from the External Examiner that no other unauthorised copies or transcripts exist.

(c) the External Examiner shall ensure that the authorised representatives who carry out the examinations or checks comply with: (a) the internal rules of the relevant Eurosystem member, as communicated to such authorised representatives before the commencement of their activity; and (b) the confidentiality obligations set out in Article 29. The External Examiner’s authorised representatives shall not enter areas or offices and shall not use physical or electronic resources of the Eurosystem other than those which are strictly needed for the performance of the examination or check.

9. The Eurosystem shall maintain documentation and records documenting the performance of this Agreement for at least 10 years after their creation and, for documents and records maintained at the date of the termination of this Agreement, for at least 10 years following the termination. Such documentation and records shall include any financial records relating to costs and expenses directly related to the performance of this Agreement, as incurred by the Eurosystem on its own behalf or on behalf of the Contracting CSD. Where the Contracting CSD notifies the Eurosystem of any potential or actual litigation requiring preservation of certain records or a change in law establishing longer documentation and records preservation periods the Eurosystem shall forthwith: (a) suspend the destruction of documentation or records, as required by the Contracting CSD; and (b) give the Contracting CSD prior written notice of at least 60 calendar days before destroying the documentation or records subject to such suspension, during which notice period the Contracting CSD may submit a reasoned request for their further maintenance, with the Eurosystem being entitled to reimbursement of reasonable costs incurred as a result of such further maintenance.

10. Nothing in paragraph 9 relieves the Contracting CSD or the Eurosystem from their statutory or contractual obligations related to the storage of records and documents.
Article 27
Governance

1. Without prejudice to Articles 8(5) and 42, the Governance framework applicable during the development and operation of T2S Services is specified in this article and, more specifically, in Schedule 8 (Governance).

2. The Eurosystem shall participate in the Governance of T2S in the performance of its tasks under the Treaty on the Functioning of the European Union and the Statute of the ESCB and in its capacity as owner and operator of T2S. In particular, this includes the ability to recover its costs and to operate T2S in a safe and efficient manner with due consideration of the rights, interests, prerogatives and obligations of the T2S Stakeholders in line with the Multilateral Character of T2S.

3. Participating CSDs shall have control and participation rights in accordance with the Governance framework of T2S, in particular through their participation in the relevant Governance bodies as set out in paragraph 4 and the decision-making process as outlined in Schedule 8.

4. Without prejudice to the ultimate decision-making powers of the Governing Council, as set out in Schedule 8, and the decision making bodies of the non-euro area NCBs, the Governance bodies shall comprise:

(a) the T2S Board, which replaces the T2S Programme Board established by Decision ECB/2009/6;

(b) the CSD Steering Group (CSG), whose mandate and composition are annexed to Schedule 8 (Governance);

(c) the Non-euro Currencies Steering Group (NECSG), whose mandate and composition are set out in Schedule 8 (Governance) of the Currency Participation Agreement;

(d) the Governors’ Forum, whose mandate and composition are part of the Schedule 8 (Governance) of the Currency Participation Agreement;

(e) the Advisory Group (AG), whose mandate and composition are set out in the Annex to Guideline ECB/2010/2 of 21 April 2010 on TARGET2-Securities; and

(f) the National User Groups (NUGs), whose mandate and composition are set out in the Annex to the Guideline ECB/2010/2 of 21 April 2010 on TARGET2-Securities. The NUGs link the respective national market with the AG.

These Governance bodies shall draft their respective rules of procedure once they have been established.
CHAPTER 4
INTELLECTUAL PROPERTY RIGHTS, CONFIDENTIALITY
AND DATA PROTECTION

Article 28
Intellectual Property Rights

1. Each Party and, where applicable, its licensors, shall retain all rights and titles in their Background IPRs. In particular, the Eurosystem shall not acquire any right, title or interest in or to the IPRs of the Contracting CSD or its licensors (including but not limited to software, CSD Static Data, Securities Reference Data, Transactional Data, data, documentation, processes, and procedures of the Contracting CSD), save to the extent required for the performance of this Agreement.

2. The Parties agree that no IPRs developed or created before or during the course of this Agreement by or for the benefit of the Eurosystem or its subcontractors shall be transferred, licensed or otherwise conveyed to the Contracting CSD, save as expressly set out in this Agreement. This includes without limitation: (a) all IPRs developed or created in connection with the development of T2S or the establishment or provision of T2S Services; (b) changes to T2S or to the T2S Scope Defining Set of Documents implemented pursuant to Change and Release Management as described in Article 25 and Schedule 9 (Change and Release Management); and (c) the T2S Documentation and any other documents created or used for the development and operations of the T2S.

3. Notwithstanding paragraph 2, the Parties may use general project know-how acquired in connection with T2S, in particular in connection with Change and Release Management, including after the termination of this Agreement.

4. The Eurosystem shall provide the T2S Services in a manner that shall ensure that no IPR of any Third Party is infringed through the use of T2S Services by the Contracting CSD in line with this Agreement. If legal action is commenced or threatened against the Contracting CSD based on an alleged infringement of the IPR of any Third Party through the use of T2S Services by the Contracting CSD, the Contracting CSD shall (a) notify the Eurosystem in accordance with Article 50 as soon as reasonably practicable; (b) allow the Eurosystem, at its expense, control of the defence of the claim (without prejudice to the Contracting CSD’s right to take an active role in the proceedings at its own expense); (c) not make admissions, agree to any settlement or otherwise compromise the defence of the claim without the prior written consent of the Eurosystem; such consent shall not be unreasonably withheld; and (d) give, at the Eurosystem’s request, reasonable assistance in connection with the conduct of the defence. If the Contracting CSD should be held legally liable for the infringement of the Third Party’s IPR according to an Enforceable Judgement or has, with the prior written consent of the Eurosystem, settled the claim, the Eurosystem shall reimburse the Contracting CSD in accordance with Schedule 13 (Procedure for payment of claims) for all payments that the Contracting CSD has to make to the relevant Third Party. The consent referred to in the previous sentence shall not be unreasonably withheld. This reimbursement obligation shall not apply with regard to any Third Party claim asserted before a court outside (a) the European Union or (b) the home country of
the Contracting CSD or any Participating CSD. In this case, the liability rules pursuant to Article 32 shall apply.

5. The Eurosystem grants to the Contracting CSD a non-exclusive and non-transferable licence to copy the T2S Documentation and any other document made available to the CSDs for any purpose connected to the use of the T2S Services or other purpose that is incidental to the rights granted to the Contracting CSD under this Agreement.

6. The T2S trademarks and logos remain the sole property of the Eurosystem. The Eurosystem grants to the Contracting CSD the non-exclusive, non-transferable right to use the T2S trademarks and logos in the territories, in which they are protected, for the T2S Services in conformity with applicable law.

7. The Contracting CSD’s trademarks and logos remain its (or its Affiliates) sole property. The Contracting CSD grants to the Eurosystem the non-exclusive, non-transferable right to use the Contracting CSD’s trademarks and logos in the territories, in which they are protected, for the T2S Services in conformity with applicable law.

Article 29
Confidentiality

1. The Parties acknowledge and agree that they have received and will receive Confidential Information in connection with this Agreement.

2. The Parties agree that all Confidential Information shall be used only for the purpose of exercising rights or complying with obligations under this Agreement and the receiving Party shall ensure that only such personnel to whom disclosure of the Confidential Information is required for the purpose of exercising any rights or the performance of the receiving Party’s obligations under this Agreement shall have access to the Confidential Information and only to the extent necessary to exercise these rights or perform these obligations.

3. To the extent that Confidential Information disclosed by a Contracting CSD consists of statistical or personal data, such data may only be used to prepare aggregated data for further use by the Eurosystem, provided that such aggregated data does not allow for the direct or indirect identification of the content of the specific Confidential Information or any personal data.

4. The receiving Party of Confidential Information shall use all reasonable efforts to protect such Confidential Information from unauthorised use or disclosure (intentional, inadvertent or otherwise) and, in any event, shall exercise at least the same reasonable level of care to avoid any such unauthorised use or disclosure as it uses to protect its Confidential Information.

5. Notwithstanding the foregoing, a receiving Party may disclose Confidential Information of the disclosing Party to Third Parties with the prior written consent of the disclosing Party,
and each Party shall be free to disclose Confidential Information without the consent of the disclosing Party only:

(a) as required by a court of competent jurisdiction or a Relevant Competent Authority or an administrative body of a competent jurisdiction, or otherwise required by the applicable laws, but only to the extent legally required;

(b) in any potential or actual litigation among the Parties arising in connection with the T2S Programme or this Agreement, to the extent required to establish, exercise or defend a legal claim;

(c) to directors, officers, personnel, attorneys, consultants, auditors, subcontractors, insurers and agents of the Contracting CSD (including persons belonging to an Affiliate of the Contracting CSD) on a strict need-to-know basis in connection with their duties, as long as such persons are advised of the confidential nature of such information and their obligation to protect it as confidential and are bound by confidentiality undertakings consistent with those contained in this Agreement,

provided that, with respect to points (a) and (c), the Party shall, subject to the applicable laws, inform the other Party reasonably in advance in writing in order to enable it to take precautionary measures.

6. If this Agreement is terminated or expires for any reason, all Parties that have received Confidential Information shall return it to the disclosing Party and/or, at the disclosing Party’s discretion, destroy it and provide a corresponding certificate to the disclosing Party, except to the extent that retention of any Confidential Information is required by applicable laws or expressly permitted under this Agreement. A receiving Party may keep one copy of the Confidential Information for backup, audit and compliance purposes, subject to the obligation to keep this copy confidential and not use the information for any other purpose. This confidentiality obligation shall remain in force following the termination or expiration of this Agreement.

7. Nothing in this Article limits the ability of the Parties to provide the text of this Agreement to the relevant Union institutions and bodies, and national authorities, including the Relevant Competent Authorities, for purposes related to receiving regulatory assessments or approvals necessary for provision and use of the T2S Services or establishing the tax status of the T2S Services.

8. The Parties acknowledge and agree that the uniform text of this Agreement may be made public (including publication on the T2S website) once the Governing Council has approved it and decided to offer this Agreement to the CSDs.

**Article 30**

**Data protection**

1. Each Party shall comply with the data protection laws applicable to it and in particular the relevant implementations of Directive 95/46/EC or, as applicable, Regulation (EC) No
2. The Eurosystem shall use personal data solely for the purpose of providing and using the T2S Services. Within these limits, the Eurosystem may transfer personal data to Third Parties including NSPs. Where the Eurosystem receives personal data from any Contracting CSD under this Agreement, and where the Eurosystem (and/or any of its subcontractors and/or Third Parties used to provide the T2S Services) transfers such personal data to a country outside the Union, which does not provide the same level of protection as in the Union, the Parties shall agree on the terms and conditions for the data transfer which shall be based on the standard contractual clauses for the transfer of personal data to processors established in third countries as approved by Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC.

3. The Contracting CSD shall acquaint itself with an NSP’s data retrieval policy prior to entering into a contractual relationship with this NSP. The Contracting CSD and, to the extent necessary under applicable law, the Eurosystem have each obtained or shall obtain all the authorisations and approvals from, or shall make the necessary notifications to, the relevant regulatory or administrative authorities as well as other interested parties (in particular the Contracting CSD’s customers) required for the Eurosystem to use and store data as contemplated under this Agreement.

CHAPTER 5
LIABILITY

Article 31
Standard of liability

1. Except as otherwise provided in this Agreement, the Parties shall be bound by a general duty of reasonable care in relation to each other in performing their obligations under this Agreement.

2. Each Party shall be obliged to perform only the duties and obligations specifically attributed to it in this Agreement and shall be liable only in respect of those duties and obligations as provided for in this Agreement.

3. Each Party shall take all reasonable and practical actions and measures to mitigate any loss, damage or adverse consequence that it may cause to the other Party or that it may suffer by reason of the acts or omissions of the other Party.

Article 32
Liability rules

1. Each Party shall be liable to the other Party without limitation for any loss or damage resulting from fraud or wilful misconduct in performing its duties and obligations under this Agreement.
T2S Framework Agreement

2. Each Party shall be liable to the other Party for any Direct Loss incurred resulting from its gross or ordinary negligence in performing its duties and obligations under this Agreement. "Direct Loss", for the purpose of this Agreement, shall mean loss or damage directly caused to the damaged Party as a result of the gross or ordinary negligence of the other Party in performing its duties and obligations under this Agreement. Lost revenues, lost profits, lost savings and reputational damage shall not qualify as Direct Loss; instead they shall qualify as indirect losses. Without prejudice to paragraphs 3 and 9, liability for indirect loss and damages not qualifying as Direct Loss is excluded to the extent permitted by German law.

3. The Eurosystem shall also be liable to the Contracting CSD for a claim of a Contracting CSD’s customer against the Contracting CSD in connection with T2S Services (hereinafter a ‘Customer Claim’), resulting from the Eurosystem’s gross or ordinary negligence in performing its duties and obligations under this Agreement, if and to the extent that all of the following criteria are satisfied: (a) the Contracting CSD has, with the approval of the Eurosystem (such approval shall not be unreasonably withheld or delayed), settled the Customer Claim or is held legally liable for the Customer Claim pursuant to an Enforceable Judgment; (b) the loss or damage of a customer is the direct result of an act or omission of the Eurosystem and (c) the Customer Claim would have been settled according to local market practice (marktübliche Bedingungen). The Contracting CSD shall reimburse to the Eurosystem a Customer Claim (i) for which the condition(s) outlined above are not fulfilled or are reversed or (ii) which is paid twice on the basis of this Agreement as well as on another basis, such as an insurance policy or through a claim paid by a Central Bank based on the same facts and circumstances. For the avoidance of doubt, no Customer Claim shall be paid directly by the Eurosystem to the Contracting CSD’s customers.

4. Each Party shall be liable to the other Party in proportion of the contribution of its fraud, willful misconduct, gross or ordinary negligence in the loss or damage of the other Party.

5. Without prejudice to paragraph 1, the Eurosystem’s liability according to this Article shall be limited or excluded as follows:

(a) The liability of the Eurosystem shall be limited to a maximum total amount per calendar year for all losses or damages suffered by the Contracting CSD and all Participating CSDs that were caused by events that occurred in the same calendar year.

   (i) In case of the Eurosystem’s ordinary negligence, the liability of the Eurosystem vis-à-vis, combined, the Contracting CSD and all Participating CSDs shall be limited to a maximum total amount of EUR 30,000,000 for the relevant calendar year.

   (ii) In case of the Eurosystem’s gross negligence, the liability of the Eurosystem vis-à-vis, combined, the Contracting CSD and all Participating CSDs shall be limited to a maximum total amount of EUR 500,000,000 for the relevant calendar year.

If the aggregate amount of losses or damages suffered by the Contracting CSD and all Participating CSDs in any calendar year exceeds the maximum set out in this subparagraph, then the amount due to the Contracting CSD shall be determined by
the Eurosystem pro rata, i.e. having regard to the total amount of all losses or damages suffered by the Contracting CSD and all Participating CSDs.

(b) The Eurosystem shall not be liable for losses or damages suffered by the Contracting CSD related to the early termination of any Parallel Framework Agreement or any Currency Participation Agreement.

(c) The Eurosystem shall have no liability for the suspension of settlement in the currency of a non-euro area NCB.

6. Without prejudice to paragraph 1, the Contracting CSD’s liability according to this Article shall be limited as follows: In the case of ordinary negligence, the liability shall be limited to the equivalent of the T2S fees that the Contracting CSD has paid during the 12 months period preceding the calendar year in which the event occurred that caused the liability claim or, in case the Contracting CSD has not paid T2S fees for 12 months, the T2S fees that the Contracting CSD could be reasonably expected to have paid during this 12 months period, taking into account the number of securities instructions that the Contracting CSD has settled in its legacy settlement infrastructure during the remainder of the 12 months period. In the case of liability due to gross negligence, the liability shall be limited to the fivefold of the amount as determined in accordance with the previous sentence.

7. If loss or damage to the Contracting CSD results from a delay of the Eurosystem in meeting synchronisation point 6 (Eurosystem ready for User Testing) according to Annex 9 of Schedule 2 (T2S Programme Planning and Monitoring), the liability of the Eurosystem shall, without prejudice to paragraph 1, not apply to a loss or damage that arises during the first 12 months of such delay.

8. If loss or damage to the Contracting CSD results from the material non-compliance of T2S with Schedule 5 (T2S Service Description) and/or the T2S Scope Defining Set of Documents, the liability of the Eurosystem shall, without prejudice to paragraph 1, not apply to a loss or damage that arises during the first 15 months following the Eurosystem’s notification of its readiness to fulfil synchronisation point 8 (Start Bilateral Interoperability Testing) according to Annex 9 of Schedule 2 (T2S Programme Planning and Monitoring).

9. If loss or damage to the Eurosystem results from a delay of the Contracting CSD in meeting its applicable synchronisation point 16 (Ready for Migration) according to Annex 9 to Schedule 2 (T2S Programme Planning and Monitoring), the liability of the Contracting CSD shall, without prejudice to paragraph 1, not apply to a loss or damage that arises during the first 12 months of such delay. After this period, the Eurosystem’s damage shall be equal to the T2S fees that the Contracting CSD could be reasonably expected to pay during the time of its delay. The Contracting CSD’s expected T2S fees shall be determined as follows: daily average number of securities instructions that the Contracting CSD settled in its legacy settlement infrastructure during the 12-months period preceding the Contracting CSD’s synchronisation point 15 according to Annex 9 of Schedule 2 (T2S Programme Planning and Monitoring) multiplied by the relevant T2S prices indicated in T2S Price List multiplied by the number of days in delay.

10. The procedures for the exercise, allocation and payment of liability claims are detailed in Section 1 of Schedule 13 (Procedure for payment of claims).
11. The right of either Party to claim damages pursuant to this Article is excluded to the extent that the Party is entitled to claim financial compensation in accordance with Article 40 for the same event.

12. For the avoidance of doubt, the circumstances specified in Article 34(1) apply as grounds for exclusion of the liability under this Article.

Article 33
Indemnification obligations of the Contracting CSD for acts of Third Parties

1. Notwithstanding Article 34(1)(b), the Contracting CSD shall indemnify and hold harmless the Eurosystem from:

(a) any claim asserted directly or indirectly against the Eurosystem by a Third Party in relation to the T2S Services used by the Contracting CSD. If legal action is commenced or threatened against the Eurosystem by a Third Party, the Eurosystem shall (a) notify the Contracting CSD in accordance with Article 50 as soon as reasonably practicable; (b) allow the Contracting CSD, at its expense, control of the defence of the claim (without prejudice to the Eurosystem’s right to take an active role in the proceedings at its own expense); (c) not make admissions, agree to any settlement or otherwise compromise the defence of the claim without the prior written consent of the Contracting CSD; such consent shall not be unreasonably withheld and (d) give, at the Contracting CSD’s request, reasonable assistance in connection with the conduct of the defence. If the Eurosystem should be held legally liable towards the Third Party according to an Enforceable Judgement or has, with the prior written consent of the Contracting CSD, settled the claim, the Contracting CSD shall reimburse the Eurosystem in accordance with Schedule 13 (Procedure for Payment of Claims) for all payments that the Eurosystem has to make to the relevant Third Party. The consent referred to in the previous sentence shall not be unreasonably withheld. This reimbursement obligation shall not apply with regard to any Third Party claim asserted before a court outside (a) the European Union or (b) the home country of the Contracting CSD or any Participating CSD. In this case, the liability rules pursuant to Article 32 shall apply;

(b) any loss or damage incurred as a result of the acts and omissions of one of the Contracting CSD’s customers in relation to T2S.

2. The obligations of the Contracting CSD pursuant to paragraph 1 shall not be construed as a limitation of any claim for loss or damage the Contracting CSD may have against the Eurosystem under this Agreement.

Article 34
Force Majeure and acts by Third Parties

1. No Party shall be responsible to the other Party for a failure to perform any of its obligations under this Agreement insofar as such failure is due to conditions beyond its reasona-
T2S Framework Agreement

The Eurosystem shall be entitled to suspend the Contracting CSD from using some or all T2S Services with immediate effect if the Relevant Competent Authority requests or supports the suspension. If the Contracting CSD is subject to an Insolvency Event or is in non-compliance with the Access Criteria, the Eurosystem, together with the Relevant Competent Authority, shall assess the required timing and level of suspension. Where possible, the suspension shall be limited to the T2S Services that are relevant to the cause of the suspension.

2. The implementation of the suspension of the Contracting CSD from using some or all T2S Services shall trigger Article 23 on Crisis management. The Eurosystem and the Contracting CSD shall use their best efforts to remove the suspension in collaboration with the Relevant Competent Authorities.

Article 36

Right of Technical Disconnection by the Eurosystem

1. The Eurosystem shall be entitled to technically disconnect the Contracting CSD from the T2S Platform with immediate effect if, in the Eurosystem’s reasonable opinion, the technical connection of the Contracting CSD to the T2S Platform represents a major threat to the security or integrity of T2S. The Technical Disconnection of the Contracting CSD may cause the Technical Disconnection of its DCPs in accordance with the Crisis management procedures. The Eurosystem shall, to the extent possible, provide reasonable prior notice of the imminent Technical Disconnection to the Relevant Competent Authorities and the Contracting CSD. Where possible, the Eurosystem shall consult the Relevant Competent Authorities prior to the Technical Disconnection.

2. The Eurosystem shall be entitled to technically disconnect a DCP from the T2S Platform with immediate effect if, in the Eurosystem’s reasonable opinion, the technical connection of such DCP to the T2S Platform represents a major threat to the security or integrity of
T2S Framework Agreement

T2S. The Eurosystem shall, to the extent possible, provide reasonable prior notice of the imminent technical disconnection of the DCP to and consult the Relevant Competent Authorities, the Contracting CSD and the DCP that is impacted.

3. The implementation of the technical disconnection of the Contracting CSD or one of its DCPs shall trigger Article 23 on Crisis management. The Eurosystem and the Contracting CSD shall undertake to use their best efforts in order to remove the disconnection after 2 hours, counting from the moment of disconnection. Where possible, the technical disconnection shall be limited to the T2S Services that are relevant to the cause of the disconnection.

Article 37
Term

1. This Agreement shall be executed on the date hereof and shall become effective on the Agreement Date. The provisions of this Agreement shall not have any retroactive effect except for Articles 6, 28 and 29, which shall apply retroactively.

2. This Agreement shall continue unless and until terminated in accordance with this Chapter. There shall be no termination rights other than those set out in this Agreement or those mandatory under applicable law.

Article 38
Termination for cause

1. The Contracting CSD shall be entitled to terminate this Agreement in the following cases:

(a) the Eurosystem is in delay of more than 18 months in meeting synchronisation point 6 (Eurosystem ready for User Testing) according to Annex 9 of Schedule 2 (T2S Programme Planning and Monitoring);  

(b) T2S does not comply in a material respect with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents and this material non-compliance is not remedied by the Eurosystem in a satisfactory manner within 15 months after the Eurosystem’s notification of its readiness to fulfil synchronisation point 8 (Start Bilateral Interoperability Testing) according to Annex 9 of Schedule 2 (T2S Programme Planning and Monitoring).

(c) after migration of the Contracting CSD, the Eurosystem is in material breach of any provision of this Agreement and this breach is not remedied within a reasonable time;

(d) after the second year following the migration of the Contracting CSD, the Eurosystem repeatedly and unreasonably refuses to implement a Specific Change.
2. The Eurosystem shall be entitled to terminate this Agreement if

   (a) the Contracting CSD does not fulfil the Access Criteria for being eligible to the T2S Services as specified in Article 5(2); or

   (b) the Contracting CSD is in material breach of any other provision of this Agreement and such breach is not remedied within a reasonable time; or

   (c) the Contracting CSD is subject to an Insolvency Event and the Eurosystem, together with the Relevant Competent Authority, has assessed the required timing for such termination; or

   (d) the provision of the T2S Services becomes illegal under existing laws or regulations.

3. Either Party shall be entitled to terminate this Agreement if

   (a) the Relevant Competent Authorities of the Contracting CSD have issued a final and binding decision which prevent the Contracting CSD from using the T2S Services or, if such decision cannot be obtained, the Contracting CSD provides evidence of the existence of legal or regulatory obstacles that make the use of the T2S Services illegal; or

   (b) the Contracting CSD does not agree with a material change approved pursuant to Article 25 and Schedule 9 (Change and Release Management) and such a change cannot be implemented as a Specific Change.

4. Prior to termination by the Eurosystem according to paragraph 2(a), the Eurosystem shall apply the following procedure for determining non-compliance of the Contracting CSD with the Access Criteria:

   (a) Where the T2S Board determines that the Contracting CSD has not complied with one or more of the Access Criteria, it shall:

      (i) evaluate the nature and seriousness of the non-compliance as well as any repeated occurrences; and

      (ii) submit a written notice informing the Contracting CSD of its conclusions regarding non-compliance.

   (b) The Contracting CSD shall respond to the T2S Board within one month of receipt of notice by providing relevant evidence.

   (c) Based on the Contracting CSD’s response, the T2S Board may, after having heard the Contracting CSD, where necessary, submit a non-compliance report to the Governing Council. It shall take into account the nature and seriousness of non-compliance by the Contracting CSD as well as any repeated occurrences.

   (d) Following receipt of the T2S Board’s non-compliance report, the Governing Council may issue a reasoned decision regarding non-compliance.
5. The Party intending to terminate this Agreement pursuant to paragraph 1 (a), (b) or 2 (b) of this Article shall first revert to the dispute resolution and escalation procedure laid down in Article 42.

6. Without prejudice to Article 41(4), the notice period which applies to this Article shall be at least 90 days. In the cases of paragraph 5, notice of termination shall only be given after the dispute resolution and escalation procedure laid down in Article 42 is completed and the issue remains unresolved.

**Article 39**

**Termination for convenience**

1. Five years after the last migration wave, the Contracting CSD shall be entitled to terminate this Agreement for convenience at any time by giving prior written notice of termination to the Eurosystem of 24 months.

2. The Contracting CSD shall also be entitled to terminate this Agreement for convenience at any time by giving prior written notice to the Eurosystem with the financial consequences stipulated in Article 40(1).

3. Five years after the last migration wave, the Eurosystem shall be entitled to terminate this Agreement for convenience at any time by giving prior written notice of termination to the Contracting CSD of 36 months.

**Article 40**

**Financial consequences of termination**

1. If this Agreement is terminated by the Eurosystem pursuant to Article 38(2)(a), (b) or (c), 38(3)(b) or by the Contracting CSD pursuant to Articles 38(1)(d), (3)(b) or 39(2), the Eurosystem shall be entitled to claim financial compensation from the Contracting CSD. The procedures for the exercise of compensation claims and for the determination of the amounts of compensation are detailed in Section 2 of Schedule 13 (Procedures for payment of Claims). In case of termination by the Contracting CSD pursuant to Article 38(1)(d), the financial compensation to be paid by the Contracting CSD in accordance with Section 2 of Schedule 13 is reduced by 50 percent.

2. If this Agreement is terminated by the Contracting CSD pursuant to Article 38(1)(a), (b) or (c), the Contracting CSD shall be entitled to claim financial compensation from the Eurosystem for the Direct Loss, as defined in Article 32(2), incurred by the Contracting CSD. The Contracting CSD claiming compensation shall provide evidence of the losses for which compensation is claimed. The procedures for the exercise of compensation claims and for the determination of the amounts of compensation, also with regard to the limitation of such claims, are detailed in Section 2 of Schedule 13 (Procedures for payment of Claims).
claims). For the avoidance of doubt, compensation for losses incurred by either Party resulting from the termination of this Agreement can be claimed only in accordance with Section 2 of Schedule 13 (Procedures for payment of Claims).

**Article 41**

**Duties of the Parties after notification of termination**

1. The Contracting CSD shall pay fees until the effective date of termination.

2. When this Agreement is terminated after the Contracting CSD has migrated to T2S, the Parties shall closely cooperate and the Eurosystem shall reasonably assist the Contracting CSD and use its best efforts in order to support the transfer of activities to the Contracting CSD itself and/or any other service provider selected by the latter. Specifically in case of termination by the Contracting CSD pursuant to Article 38(3)(a), the Eurosystem shall deploy additional assistance and efforts to achieve the objectives stated in this Article.

3. The details of the cooperation and assistance to be provided by the Eurosystem are specified in Schedule 11 (Exit Management) and are based on the following principles:

   (a) the Contracting CSD is responsible for the set up and execution of the exit plan; and

   (b) the Eurosystem shall provide the required assistance, as reasonably necessary, to the Contracting CSD.

4. Without prejudice to the termination rights of the Eurosystem pursuant to Article 38(2)(a), (b), (c) and (d), 38(3)(a) and (b), the Eurosystem shall, upon request of the Contracting CSD, continue to provide the T2S Services to the Contracting CSD for a period of up to 24 months after the date of the service of notice of termination, but not beyond the effectiveness of such termination, as long as the Contracting CSD complies with the T2S Access Criteria. In case the Contracting CSD cannot comply with all Access Criteria, the Parties, together with the Relevant Competent Authority, shall assess the required level of provision of T2S Services.

5. The Eurosystem shall maintain at the disposal of the Contracting CSD the relevant documents, data and archives related to T2S Services provided to the Contracting CSD.

6. From the date of notification of termination, the Contracting CSD shall become an observer in the entities or bodies governing T2S in which it participated. As an observer, the Contracting CSD shall not be entitled to vote, unless decisions relate to the day-to-day management and operation of T2S. From the effectiveness of termination, the Contracting CSD shall be excluded from any entities or bodies governing T2S.
CHAPTER 7
MISCELLANEOUS

Article 42
Dispute resolution and escalation

1. The Eurosystem and the Contracting CSD shall attempt to resolve disputes involving: (a) the Eurosystem and the Contracting CSD, or, as the case may be, (b) the Eurosystem, the Contracting CSD and one or more Participating CSDs, and which arise out of or relate to this Agreement, any Parallel Framework Agreements or the provision or use of the T2S Services, in a constructive manner that reflects their respective concerns and legitimate interests. The first attempt to resolve a dispute shall be, as soon as the circumstances allow, through negotiations between the Eurosystem, the Contracting CSD and, as the case may be, the involved Participating CSDs.

2. If the attempt to resolve a dispute through negotiations is unsuccessful, the Eurosystem, the Contracting CSD or any Participating CSD involved in the dispute may escalate the matter to the CSG. The CSG shall attempt to resolve the dispute and find a mutually agreeable solution within 60 calendar days from the date of the first meeting of the CSG in which the dispute was discussed. The CSG may establish a Resolution Task Force, grouping representatives of the Eurosystem and of the CSDs involved, selected with the view to ensuring balanced representation of the whole CSG.

3. If no mutually agreeable solution can be reached by the CSG, the issue may be escalated to the T2S Board. Any party to the dispute may address the T2S Board with submissions in writing. The T2S Board shall deliver its proposal for the resolution of the matter within 60 calendar days after the dispute has been submitted to the T2S Board in writing to the parties involved.

4. If the parties involved in the dispute do not agree to the resolution proposal made by the T2S Board, they shall notify the T2S Board within 60 calendar days and the T2S Board Chairperson shall without delay inform the Governing Council of this outcome. The T2S Board Chairperson shall make a reasoned proposal of the resolution options to the Governing Council, documenting the status of the dispute and the positions of the Eurosystem, the Contracting CSD and, if applicable, the Participating CSDs. Any party to the dispute may address the Governing Council with submissions in writing. As a result of its review, the Governing Council shall decide on the resolution of the dispute within a reasonable time.

5. At any point of the procedure described in paragraphs 1 to 4, advice on the disputed issues from the Advisory Group and the NECSG may be requested by the T2S Board Chairperson, by the Contracting CSD, by any Participating CSD involved in the dispute, by the CSG, and by the Governing Council. The Advisory Group and the NECSG shall provide their advice without delay and in due time for it to be considered before the escalation procedure is concluded or moved to the next stage. The Advisory Group and the NECSG may request at any stage of the escalation procedure an appropriate prolongation of the time for giving their respective advice, if necessary for the adequate preparation of the advice.
T2S Framework Agreement

6. At each stage of the escalation process, adequate consideration shall be given to related matters that are the subject of similar escalation procedures between the Eurosystem and a non-euro area Central Banks in T2S.

Article 43
Arbitration

1. The Parties agree that any dispute between the Parties arising out of or in connection with this Agreement shall be decided through proceedings between all Parties to this Agreement and that any dispute shall, subject to the prior completion of the dispute resolution and escalation procedure set out in Article 42, be brought before the Court of Justice of the European Union by either of the Parties in accordance with Article 35.4 of the Statute of the ESCB.

2. The members of the Eurosystem can internally agree to authorise a Eurosystem Central Bank to act in the name and on behalf of all the other members of the Eurosystem in all matters related to an Arbitration arising under this Article. Any such agreement shall promptly be communicated by the Eurosystem to the Contracting CSD.

Article 44
Own fees and costs

Each Party shall bear its own costs and expenses connected with the preparation, execution and application of this Agreement (including the costs of its legal and other advisors), without prejudice to other provisions of this Agreement.

Article 45
Public announcements

Without prejudice to Articles 8 and 29(7), the Parties shall not issue nor allow for any press releases or communications relating to the performance or non-performance of either Party under this Agreement without the prior written approval of the other Party.

Article 46
Entire Agreement and non-retroactivity

The Agreement and the Schedules represent the complete agreement regarding the subject-matter hereof and replace any prior oral or written communications between the Eurosystem and the Contracting CSD, including those resulting from the T2S Memorandum of Understanding.
1. Any amendment of, or supplement to, this Agreement must be executed in writing and agreed by both Parties unless provided otherwise in this Article. Written form in the meaning of this Article requires a formal document containing the amendment or supplement with a statement that the document is intended to amend or supplement this Agreement. The document shall be duly signed by Authorised Representatives of the Parties.

2. The Eurosystem shall notify the CSG of its intention to amend the Schedules with regard to minor changes of a technical or operational nature. These minor changes shall be deemed to be approved unless the CSG or the Contracting CSD, within 21 calendar days, notifies the Eurosystem that in its view such changes may not be considered minor. In the latter case, the amendment procedure according to paragraph 1 shall apply.

3. The Parties agree to negotiate in good faith to amend this Agreement, to the extent required, in the event that any of the legal acts or instruments forming an element of the overall legal framework for T2S, including for the avoidance of doubt any relevant legal act or instrument that applies in the jurisdiction of the Contracting CSD, is amended and in the event any such amendment has a material effect on this Agreement in the reasonable opinion of the Eurosystem or of the Contracting CSD.

4. The Parties shall implement the system changes decided pursuant to Article 24 and Schedule 9 (Change and Release Management). The scope of system changes is further defined in Schedule 9 (Change and Release Management).

5. The Eurosystem may, except as provided otherwise under paragraph 6 and subject to paragraph 4 regarding system changes, amend the Annexes to the Schedules, with the CSG’s agreement.

6. The Eurosystem may amend the Annexes to Schedule 2 (T2S Programme Planning and Monitoring) pursuant to the process detailed therein. Furthermore, the Eurosystem may amend Schedule 7 (Pricing), with prior notice of 180 calendar days to the Contracting CSD, in accordance with the T2S pricing policy decided by the Governing Council and published on the T2S’s website or if the actual usage of T2S Services that have an initial zero price is not within an expected consumption pattern. This is without prejudice to the account management service fee for securities accounts which will be kept at zero until the end of the cost recovery period and which the Eurosystem may only amend with prior notice of 24 months to the Contracting CSD.

**Article 48**

**No waiver**

The exercise or waiver, in whole or in part, of any right, remedy, or duty provided for in this Agreement shall not constitute the waiver of any prior, concurrent or subsequent right, remedy, or duty within this Agreement.
Article 49
Survival

Any terms of this Agreement that by their nature extend beyond its expiration or termination shall remain in effect until fulfilled, including those concerning examination and records retention, Confidential Information, Arbitration, governing law and jurisdiction, indemnification, Intellectual Property Rights, limitation of liability, limitations period, charges, credits and payments, survival, and warranty.

Article 50
Notices

All notices to be given or other communications to be made pursuant to this Agreement shall be valid only if made in writing, including e-mail or facsimile transmission, to the Authorised Representative notified as such by the other Party.

Except as otherwise provided for in the MOP, all notices of the Contracting CSD to the Eurosystem in relation to this Agreement shall be submitted to the entity having executed this Agreement on behalf of the Eurosystem.

Article 51
Invalid or incomplete provisions

If a provision of this Agreement is or becomes invalid or is inadvertently incomplete, the validity of the other provisions of this Agreement shall not be affected thereby. The invalid or incomplete provision shall be replaced or supplemented by a legally valid provision that is consistent with the Parties intentions or with what would have been the Parties intentions according to the aims of this Agreement had they recognised the invalidity or incompleteness. It is the Parties’ intention that this Article shall not merely result in a reversal of the burden of proof but that Section 139 of the BGB is contracted out in its entirety.

Article 52
No agency or transfer of undertaking

1. Except for the [insert the name of the acting euro area NCB/ECB] acting in the name and on behalf of the Eurosystem, this Agreement shall not be construed to deem either Party as a representative, agent, employee, partner, or joint venturer of the other Party. The Eurosystem shall not have the authority to enter into any agreement, nor to assume any liability, on behalf of the Contracting CSD, nor to bind or commit the Contracting CSD in any manner, except as provided hereunder.
T2S Framework Agreement

2. Nothing in this Agreement shall be construed as a transfer of the Contracting CSD’s undertaking, or any part thereof, including any employment contracts, to the Eurosystem.

Article 53

Joint liability

As part of the Eurosystem’s tasks in accordance with Articles 17, 18 and 22 of the Statute of the ESCB and of the ECB, T2S has the nature of a public service. All obligations of the Eurosystem arising under this Agreement can only be performed jointly by all members of the Eurosystem and qualify as a joint liability. All rights and claims of the Contracting CSD under this Agreement are therefore always rights and/or claims that can be exercised only against all members of the Eurosystem jointly.

Article 54

Choice of law

The Agreement shall be governed by the laws of Germany.

[Signature page(s) follow(s).]
T2S Framework Agreement

Signed in [Frankfurt am Main] for and on behalf of:

[● Insert name of the acting euro area NCB/ECB], acting in the name and on behalf of the Eurosystem

_____________________________   ___________________________
(Signature)                  (Signature)

___________________________   ___________________________
(Name)                     (Name)
Date:  ____________________

Signed for and on behalf of:

[● Insert name of the Contracting CSD]

_____________________________   ___________________________
(Signature)                  (Signature)

___________________________   ___________________________
(Name)                     (Name)
Date:  ____________________
FRAMEWORK AGREEMENT

SCHEDULE 1

DEFINITIONS
1 Definitions

In this Agreement, unless the context requires otherwise, terms defined in the singular have the same meaning in the plural, and vice versa.

In this Agreement, references to Union legislation are intended as referring to the most recent version of that legal act.

In this Agreement, unless the context requires otherwise, terms with an initial capital letter have the following meanings:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘4CB’</td>
<td>means the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d’Italia, collectively, in their capacity as national central banks (NCBs) responsible for building, maintaining and running the T2S Platform based on the relevant contractual arrangements and on decisions of the Governing Council.</td>
</tr>
<tr>
<td>‘Access Criteria’</td>
<td>means the access criteria for Central Securities Depositories (CSDs) wishing to use the T2S Services, as set out in Article 15 of Guideline ECB/2012/13. These are also referred to as the eligibility criteria, as adopted by the ECB Governing Council on 14 January 2010.</td>
</tr>
<tr>
<td>‘Advisory Group (AG)’</td>
<td>means the T2S Advisory Group, the mandate and composition of which is set out in the Annex to Guideline ECB/2012/13.</td>
</tr>
<tr>
<td>‘Affiliate’</td>
<td>means a legal entity which, with respect to any person, directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with the person in question. For the purposes of this definition, ‘control’ means the possession, directly or indirectly, of more than 50% of the equity interests of a person or the power to direct or cause the direction of the management and policies of a person, in whole or in part, whether through ownership of voting interests, by contract or otherwise.</td>
</tr>
<tr>
<td>‘Agreement’ or ‘Framework Agreement (FA)’</td>
<td>means the contractual arrangement composed of a core agreement, including Schedules and Annexes, between a Contracting CSD and the Eurosystem.</td>
</tr>
<tr>
<td>‘Agreement Date’</td>
<td>means the date on which both contracting parties signed this Agreement.</td>
</tr>
<tr>
<td>‘Annex’</td>
<td>means an Annex to one of the Schedules of this Agreement.</td>
</tr>
<tr>
<td>‘Application-to-Application (‘A2A’)’</td>
<td>means a connectivity mode to exchange information between the T2S software application and the application(s) at the T2S Actor.</td>
</tr>
<tr>
<td>‘Arbitration’</td>
<td>has the meaning set out in Article 43 of this Agreement.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>‘Authorised Representative’</td>
<td>means the individual appointed by either party to such role and notified to the other party in accordance with Article 47 of this Agreement.</td>
</tr>
<tr>
<td>‘Background IPRs’</td>
<td>means all IPRs owned by or licensed to the Contracting CSD or the Eurosystem prior to the Agreement Date.</td>
</tr>
<tr>
<td>‘Basic Custody Service’</td>
<td>means the holding and administration of securities and other financial instruments, by an entity entrusted with such tasks. Basic Custody Service includes the safekeeping of securities, the distribution of interest and dividends on the securities in safekeeping, and the processing of corporate actions on the said securities.</td>
</tr>
<tr>
<td>‘Batch Settlement’</td>
<td>means the set of sequenced, scheduled processes in T2S that settle or attempt to settle all instructions that are eligible for settlement on a transaction-by-transaction basis.</td>
</tr>
<tr>
<td>‘BGB’</td>
<td>means the Bürgerliches Gesetzbuch (the German Civil Code).</td>
</tr>
<tr>
<td>‘Business Continuity and Disaster Recovery’</td>
<td>means the set of rules and procedures aimed at resuming normal T2S Services in compliance with the Service Levels as described in Schedule 6 (T2S Service Level Agreement), after the occurrence of an incident, as well as at mitigating the impact of such an incident.</td>
</tr>
<tr>
<td>‘Central Bank (CB)’</td>
<td>means the European Central Bank (ECB), the euro area NCBs and the non-euro area NCBs.</td>
</tr>
<tr>
<td>‘Central Bank Money (CeBM)’</td>
<td>means the liabilities of a Central Bank, in the form of either banknotes or bank deposits held at a Central Bank, which can be used for settlement purposes.</td>
</tr>
<tr>
<td>‘Central Securities Depository (CSD)’</td>
<td>means an entity that a) enables securities to be established and settled in book entry form, and/or maintains and administers securities on behalf of others through the provision or maintenance of securities accounts; and b) operates or provides for a Securities Settlement System in accordance with Article 2(a) of Directive 98/26/EC or for entities not located in the EEA in accordance with the relevant national legislation equivalent with Directive 98/26/EC and/or that is regulated by Central Bank; and c) is recognised as a CSD by national regulations and/or legislation and/or authorised or regulated as such by the Relevant Competent Authority.</td>
</tr>
<tr>
<td>‘Change and Release Management (CRM)’</td>
<td>means the set of rules used and the activities performed when a Change Request, as described in Schedule 9 (Change and Release Management) is initiated and until it is rejected or the change is implemented into the production environment.</td>
</tr>
<tr>
<td>‘Change Management’</td>
<td>means the processes used and the activities performed when a Change Request as described in Schedule 9 (Change and Release Management) is initiated and until it is rejected or authorised for implementation.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>‘Change Request’</td>
<td>means a request of a contracting party for a change that is subject to the Change and Release Management process, as described in Schedule 9 (Change and Release Management).</td>
</tr>
<tr>
<td>‘Change Review Group (CRG)’</td>
<td>means the group established by the Steering Level and composed of the relevant T2S Actors mandated to analyse Change Requests and make proposals on the content of T2S releases, as further specified in Schedule 9 (Change and Release Management).</td>
</tr>
<tr>
<td>‘Common Change’</td>
<td>means a change implemented for the benefit of all T2S Actors as described in Schedule 9 (Change and Release Management).</td>
</tr>
<tr>
<td>‘Common Static Data’</td>
<td>means the business information, which is available to all T2S Actors and which T2S requires to process business operations. This includes but is not limited to processing schedules, system entities, the SWIFT BIC Directory, system configuration data, attribute domains that are not specific to a CSD or Central Bank and standardised roles and privileges from which CSDs and Central Banks can configure their specific roles and access rights for their system users.</td>
</tr>
<tr>
<td>‘Confidential Information’</td>
<td>means any information, data, documentation or material that includes trade and business secrets, know-how and information regarding the business, strategy, financial situation, products and prospects, processes and methodologies, customers, suppliers and employees, systems, programs, algorithms, source codes, technical and security requirements and specifications (including any information that any party is obliged to keep confidential according to a contractual agreement or by law), and any other information, material or documentation (in each case to the extent marked as confidential or with a similar designation, or which a reasonable person would consider as confidential) related to a party or its Affiliates, which such a party has disclosed (in whatever form) to the other party in connection with this Agreement. Confidential Information does not include information that: (a) has been designated by a party as being intended for disclosure to Third Parties and does not reveal Confidential Information received by another party; (b) becomes generally available to the public other than as a result of a breach of the confidentiality obligations under this Agreement; or (c) is received from a Third Party not bound by an obligation of confidentiality with respect to such information (while the receiving party is aware or made aware by the other party of this fact); (d) was known to or legally in a party’s possession without obligations of confidentiality prior to such information being provided as Confidential Information in accordance with this Agreement; or (e) is developed by either party (or its Affiliates or their employees or representatives) independently without the use of Confidential Information of the other party.</td>
</tr>
<tr>
<td>‘Connectivity Services’</td>
<td>means the combination of Physical Connectivity Services and Value-added Connectivity Services.</td>
</tr>
<tr>
<td>‘Contracting CSD’</td>
<td>means the CSD which enters into this Agreement.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>‘Crisis’ or ‘Crisis Situation’</td>
<td>means a situation that requires the involvement of the senior manager of the Contracting CSD (referred to as CSD crisis manager in Schedule 6 [T2S Service Level agreement]), in order to manage a severe technical incident or market disturbance, either in accordance with the requirements specified in the MOP or because the procedures described in the MOP are not sufficient to effectively handle the situation.</td>
</tr>
<tr>
<td>‘CSD Static Data’</td>
<td>means the business information, specific to a CSD in T2S that T2S requires to process the Transactional Data related to that CSD. This includes but is not limited to T2S system users, conditional securities parameters, message subscriptions, attribute domains that are specific to the CSD or relevant Central Bank, report subscriptions, securities account reference data, party reference data, cross-CSD settlement parameterisation, assignment of securities accounts to limits, and CSD-specific attributes for Securities Reference Data.</td>
</tr>
<tr>
<td>‘CSD Steering Group (CSG)’</td>
<td>means the T2S governance body which, with respect to a set of matters stipulated in this Agreement, is part of the Steering Level and makes resolutions and delivers opinions on behalf of the Contracting CSD and the Participating CSDs. The CSG mandate is annexed to Schedule 8 (Governance).</td>
</tr>
<tr>
<td>‘CSDs’ Acceptance Tests of the T2S Services’</td>
<td>means the process whereby the Contracting CSD assesses the compliance of T2S with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents as further specified in Article 17 of this Agreement and in Schedule 3 (User Testing).</td>
</tr>
<tr>
<td>‘Currency Participation Agreement (CPA)’</td>
<td>means each of the contractual agreements to be entered into by the Eurosystem and a non-euro area NCB or another authority responsible for a non-euro currency, to allow for securities settlement in Central Bank Money in the non-euro currency they are responsible for.</td>
</tr>
<tr>
<td>‘Customer Claim’</td>
<td>has the meaning set out in Article 32 of this Agreement.</td>
</tr>
<tr>
<td>‘Dedicated Cash Account (DCA)’</td>
<td>means a cash account in T2S operated by a Central Bank.</td>
</tr>
</tbody>
</table>
**Schedule 1 – Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Dedicated Link Connection’</td>
<td>means a solution to connect the T2S data centres with the data centres of the Directly Connected T2S Actors, whereby the Value-added Connectivity Services are implemented in T2S and in the systems of the Directly Connected T2S Actors.</td>
</tr>
<tr>
<td>‘Delivery versus Payment (DvP)’</td>
<td>means a securities settlement mechanism, which links a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if – and only if – the corresponding payment occurs.</td>
</tr>
<tr>
<td>‘Development Phase’</td>
<td>means the period during which the Eurosystem specifies, develops and tests T2S and establishes its operational framework; this period ends on the date that the Governing Council decides that the full scope of T2S Services as documented in Schedule 5 (T2S Service Description) are operational in the T2S production environment, as depicted in Annex 1 (Diagram of Phases/Periods) to this Schedule.</td>
</tr>
<tr>
<td>‘Direct Loss’</td>
<td>has the meaning set out in Article 32(2) of this Agreement.</td>
</tr>
<tr>
<td>‘Directly Connected Party (DCP)’</td>
<td>means a T2S User, which has been authorised by its Contracting CSD or Central Bank to access T2S directly to use T2S Services, i.e. without the need for the Contracting CSD to act as a technical interface.</td>
</tr>
<tr>
<td>‘Directly Connected T2S Actor’</td>
<td>means either the Contracting CSD or any of the Participating CSDs, or any of the connected NCBs, or any of the DCPs.</td>
</tr>
<tr>
<td>‘Dynamic Data’</td>
<td>see ‘Transactional Data’.</td>
</tr>
<tr>
<td>‘Enforceable Judgement’</td>
<td>means a binding and enforceable judgment or equivalent type of decision rendered by a court or award rendered by an arbitral tribunal.</td>
</tr>
<tr>
<td>‘euro area NCB’</td>
<td>means the NCB of a Union Member State whose currency is the euro.</td>
</tr>
<tr>
<td>‘European System of Central Banks (ESCB)’</td>
<td>means, in accordance with Article 282(1) of the Treaty on the Functioning of the European Union, the System constituted by the ECB and the NCBs of the Union Member States.</td>
</tr>
<tr>
<td>‘Eurosystem’</td>
<td>means, in accordance with Article 1 of the Statute of the ESCB and of the European Central Bank, the ECB and the NCBs of the Union Member States whose currency is the euro.</td>
</tr>
<tr>
<td>‘Eurosystem Acceptance Testing (EAT)’</td>
<td>means the formal testing conducted by the Eurosystem to determine whether the T2S Platform is compliant with the T2S Scope Defining Set of Documents.</td>
</tr>
<tr>
<td>‘Exit Management’</td>
<td>means the set of rules and procedures applied on termination of the Agreement, howsoever caused, as described in Schedule 11 (Exit Management).</td>
</tr>
</tbody>
</table>
### Schedule 1 – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘External Examiner’</td>
<td>means a well-reputed, internationally active auditing firm that has the tasks set out in Article 26 of this Agreement assigned to it.</td>
</tr>
<tr>
<td>‘Fast-track Changes’</td>
<td>means changes that are imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management, or changes that are critical for the stability of the T2S Platform or by Central Bank decisions related to safeguarding the currencies or related to crisis management measures to ensure financial stability and that, owing to the time constraints, have to be implemented in a shorter timeframe than normal, which will be decided on an ad-hoc basis, as specified in Schedule 9 (Change and Release Management).</td>
</tr>
<tr>
<td>‘Force Majeure’</td>
<td>means any circumstances beyond the reasonable control of the non-performing contracting party, including, without limitation, an element of nature or an act of God, earthquake, fire, flood, war, terrorism, civil, industrial or military disturbance, sabotage, labour strike or lock-outs, pandemic, epidemic, riot, loss or malfunction of utilities or communication services, court order, act of civil or military authority, or governmental, judicial or regulatory action.</td>
</tr>
<tr>
<td>‘Framework Agreement’</td>
<td>see ‘Agreement’.</td>
</tr>
<tr>
<td>‘Free of Payment (FoP)’</td>
<td>means the delivery of securities with no corresponding payment.</td>
</tr>
<tr>
<td>‘General Specifications (GS)’</td>
<td>means together with the GFS and the GTD, the document that describes how the Eurosystem envisages implementing the URD. In particular, the General Specifications focus on those user requirements that do not have a functional or technical dimension, such as operational support, testing, migration and Information Security.</td>
</tr>
<tr>
<td>‘General Functional Specifications (GFS)’</td>
<td>means a general functional description of the T2S Business Application to be developed to comply with the URD. It will include elements such as the functional architecture (domains, modules and interactions), the conceptual models, the data model or the data flow process.</td>
</tr>
<tr>
<td>‘Governance’</td>
<td>means the set of rules and procedures concerning the management of T2S Services, including the related decision-making of the parties involved in T2S, as specified in Schedule 8 (Governance).</td>
</tr>
<tr>
<td>‘Governing Council’</td>
<td>means the decision-making body of the ECB comprising the members of the Executive Board of the ECB and the governors of the euro area NCBs, as provided for in Article 10 of the Statute of the ESCB.</td>
</tr>
<tr>
<td>‘General Technical Design (GTD)’</td>
<td>means the document that details the solution envisaged for the T2S non-functional requirements, more specifically with regard to the application design and the infrastructure design.</td>
</tr>
</tbody>
</table>
### Schedule 1 – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Graphical User Interface (GUI)’</td>
<td>means the interface that allows a user to interact with a software application through the use of graphical elements (e.g. windows, menus, buttons and icons) on a computer screen using the keyboard and the mouse.</td>
</tr>
<tr>
<td>‘Information Technology Infrastructure Library (ITIL)’</td>
<td>means the set of best practices for managing IT infrastructure, development and operations, maintained under the auspices of the Office of Government Commerce, an office of the UK Treasury.</td>
</tr>
<tr>
<td>‘Insolvency Event’</td>
<td>means a collective judicial or administrative proceeding, including an interim proceeding, in which the assets and affairs of the Contracting CSD are subject to control or supervision by a court or other competent authority for the purpose of reorganisation, winding up or liquidation.</td>
</tr>
<tr>
<td>‘Intellectual Property Rights (IPRs)’</td>
<td>means any patents, utility models, designs, trademarks, copyrights (each of the foregoing, to the extent applicable, registered, applied for or unregistered), inventions whether or not patentable, database rights, know-how and all rights having equivalent or similar effect in any jurisdiction.</td>
</tr>
<tr>
<td>‘Intended Settlement Date (ISD)’</td>
<td>means the date on which the parties to a securities transaction agree that settlement is to take place. The ISD is also referred to as the contractual settlement date or value date.</td>
</tr>
<tr>
<td>‘International Securities Identification Number (ISIN)’</td>
<td>means the number, which uniquely identifies a security. Its structure is defined in ISO 6166.</td>
</tr>
<tr>
<td>‘Investor CSD’</td>
<td>means a CSD that holds a security for which it is not the/an Issuer CSD. It holds these securities either directly or indirectly, via one or more intermediaries, at the/an Issuer CSD.</td>
</tr>
<tr>
<td>‘Issuer CSD’</td>
<td>means a CSD, which holds a primary deposit in the relevant securities, either in dematerialised or physical form.</td>
</tr>
<tr>
<td>‘Key Performance Indicator(s) (KPI(s))’</td>
<td>means a metric used to quantify the performance of the Eurosystem and to monitor compliance with the Service Level Agreement.</td>
</tr>
<tr>
<td>‘Lean Scope of T2S’</td>
<td>means the scope of T2S defined by the URD resulting from the market involvement and is restricted by the General Principles of T2S, as referenced in the URD.</td>
</tr>
<tr>
<td>‘Legal and Regulatory Requirements’</td>
<td>means all applicable requirements that a Contracting CSD and the Eurosystem must comply with, including those of a legal, regulatory (including fiscal), supervisory and oversight nature and that are relevant in the context of T2S.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>‘Licence Agreement’</td>
<td>means the contract signed by the Banca d’Italia in the name and on behalf of the Eurosystem and each NSP, which contains the requirements which the latter has to fulfil to be entitled to deliver the Connectivity Services to the Eurosystem and to the Directly Connected T2S Actors.</td>
</tr>
<tr>
<td>‘Maintenance Window’</td>
<td>means the period for system maintenance during which T2S is planned to be unavailable, as defined in Schedule 6 (Service Level Agreement).</td>
</tr>
<tr>
<td>‘Manual of Operational Procedures (MOP)’</td>
<td>means the document that describes the procedures to be applied by all T2S Actors, aimed at ensuring the smooth conduct of daily operations and at minimising the duration and impact of service interruptions or deteriorations.</td>
</tr>
<tr>
<td>‘Matching’</td>
<td>means the process used for comparing the settlement details provided by parties in order to ensure that they agree on the terms of the transaction.</td>
</tr>
<tr>
<td>‘Migration’</td>
<td>means a set of rules and procedures concerning the Contracting CSD’s migration to T2S, as described in Schedule 4 (Migration).</td>
</tr>
<tr>
<td>‘Migration Period’</td>
<td>means the time frame beginning on the date on which the T2S Board confirms that the T2S production environment is ready for CSDs and Central Banks to connect (SP14.1 - Ready to connect to Production (Wave 1)) and ending on the date on which all Contracting and Participating CSDs have migrated to T2S.</td>
</tr>
<tr>
<td>‘Multilateral Character of T2S’</td>
<td>has the meaning set out in Article 4 of this Agreement.</td>
</tr>
<tr>
<td>‘Network Service Provider (NSP)’</td>
<td>means a network service provider (NSP) that has concluded a Licence Agreement with the Eurosystem to provide Connectivity Services to T2S. It is a business or organisation providing the technical infrastructure, including hardware and software, to establish a secure and encrypted network connection that permits the exchange of information between T2S Actors and T2S.</td>
</tr>
<tr>
<td>‘non-euro area NCB’</td>
<td>means the NCB of a Union Member State, whose currency is not the euro, or of a country that is outside the Union.</td>
</tr>
<tr>
<td>‘Non-euro Currencies Steering Group (NECSG)’</td>
<td>means the T2S governance body which, with respect to a set of matters stipulated in the CPAs, makes resolutions and delivers opinions on behalf of the non-euro area NCBs having signed the CPA. The NECSG mandate is annexed to Schedule 8 (Governance) of the CPA.</td>
</tr>
<tr>
<td>‘Operations Managers Group (OMG)’</td>
<td>means the group established by the Steering Level and composed of the relevant T2S Actors that develops and maintains the Manual of Operational Procedures, meets to review the T2S service performance against the Service Level Agreement and coordinates the management of operational incidents, as specified in Schedule 6 (T2S Service Level Agreement).</td>
</tr>
<tr>
<td>‘Operational Phase’</td>
<td>means the period when the full scope of T2S Services are operational in the T2S production environment, and beginning on the T2S Go-Live Date, as depicted in Annex 1 to this Schedule.</td>
</tr>
<tr>
<td>‘Other T2S Specification Documents’</td>
<td>means the set of documents, when added to the T2S Scope Defining Set of Documents, that provide a full description of T2S. This includes the GFS non-Functional Chapters.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>‘Parallel Framework Agreement’</td>
<td>means an agreement essentially identical, save for the identity of the parties to the agreement entered into between a Participating CSD and the Eurosystem.</td>
</tr>
<tr>
<td>‘Participating CSD(s)’</td>
<td>means the CSD(s) other than the Contracting CSD that have signed this Agreement.</td>
</tr>
<tr>
<td>‘Payment Bank’</td>
<td>means a commercial bank used to effect money settlements. In the context of securities settlement, a Payment Bank provides cash on behalf of a CSD participant to support the settlement of securities.</td>
</tr>
<tr>
<td>‘Payment Free of Delivery (PFoD)’</td>
<td>means a transfer of cash without the delivery of securities.</td>
</tr>
<tr>
<td>‘Physical Connectivity Services’</td>
<td>means the implementing, maintaining and keeping available of a data communication network for the purpose of exchanging files and messages between the Directly Connected T2S Actors and T2S, as more specifically described in the Licence Agreement.</td>
</tr>
<tr>
<td>‘Project Managers Group (PMG)’</td>
<td>means the group established by the Steering Level and composed of the relevant T2S Actors that coordinates and monitors activities to ensure that the initial release as well as subsequent releases of T2S go live, as specified in Schedule 2 (T2S Programme Planning and Monitoring), 3 (User Testing) and 4 (Migration).</td>
</tr>
<tr>
<td>‘Pricing’</td>
<td>means the set of rules and procedures that is applied to price the T2S Services and T2S-related services provided by the Eurosystem, as described in Schedule 7 (Pricing).</td>
</tr>
<tr>
<td>‘Real-time Settlement’</td>
<td>means the continuous process in T2S that settles or attempts to settle instructions that are eligible for settlement on a transaction-by-transaction basis.</td>
</tr>
<tr>
<td>‘Release Management’</td>
<td>means the set of rules used and the activities performed to implement a set of authorised changes and defect corrections in a new version of the T2S Business Application, as set out in Schedule 9 (Change and Release Management).</td>
</tr>
<tr>
<td>‘Relevant Competent Authority’</td>
<td>means any organisation having regulatory, supervisory or oversight authority over the Contracting CSD or a Participating CSD (as required by the context).</td>
</tr>
<tr>
<td>‘Schedule’</td>
<td>means a Schedule to this Agreement.</td>
</tr>
<tr>
<td>‘Securities Account’</td>
<td>means an account maintained by a CSD to which securities may be credited or debited.</td>
</tr>
<tr>
<td>‘Securities Maintaining Entity (SME)’</td>
<td>means an entity, typically a CSD that has been assigned the responsibility for maintaining the reference data for a security in T2S.</td>
</tr>
</tbody>
</table>
### Schedule 1 – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Securities Reference Data’</td>
<td>means the business information for a financial instrument, excluding any CSD-specific attributes and under the responsibility of the SME and available to all Participating CSDs, that T2S stores and requires for processing all operations related to settlement instructions.</td>
</tr>
<tr>
<td>‘Securities Settlement System’</td>
<td>means a system as defined in Article 2(a) of Directive 98/26/EC for the execution of transfer orders related to title to or interest in a security or securities by means of a book entry on a register or otherwise.</td>
</tr>
<tr>
<td>‘Service Description’</td>
<td>means the description of the T2S Services, contained in Schedule 5 (T2S Service Description).</td>
</tr>
<tr>
<td>‘Service Level’</td>
<td>means the level of performance of a T2S Service, that Schedule 6 (T2S Service Level Agreement) specifies and that the Contracting CSD requires to deliver its services to its customers.</td>
</tr>
<tr>
<td>‘Service Level Agreement (SLA)’</td>
<td>means the agreement defining the Service Levels, measured against agreed KPIs where relevant, to be provided by the Eurosystem to the CSDs, as specified in Schedule 6 (T2S Service Level Agreement) and in relation to T2S Services.</td>
</tr>
<tr>
<td>‘Service Level Report’</td>
<td>means the monthly report made available by the Eurosystem to the Contracting CSD to determine the degree of the Eurosystem’s compliance with the Service Level Agreement, as specified in Schedule 6 (T2S Service Level Agreement), in particular as regards the KPIs.</td>
</tr>
<tr>
<td>‘Settlement Day’</td>
<td>means a day on which T2S settlement takes place according to the daily processing schedule.</td>
</tr>
<tr>
<td>‘Specific Change’</td>
<td>means any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is not implemented as a Common Change (within the applicable Governance arrangements), but which some Participating CSDs and/or Central Banks wish to implement, provided that it is compliant with the Lean Scope of T2S, and for which they jointly accept to bear the investment and running costs.</td>
</tr>
<tr>
<td>‘Steering Level’</td>
<td>means the level comprising the T2S Board for tasks delegated by the Governing Council, the CSG and the NECSG, as specified in Schedule 8 (Governance).</td>
</tr>
<tr>
<td>‘Suspension’</td>
<td>means the temporary freezing – possibly limited to the T2S Services relevant to the cause of suspension – of the rights and obligations of the Contracting CSD for a period of time to be determined by the Eurosystem, as described in Article 35.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>‘T2S Actor’</td>
<td>means either the Contracting CSD, a Participating CSD, CSD participant (a legal entity or, as the case may be, an individual) having a contractual relationship with the CSD for the processing of its securities settlement-related activities in T2S, or a Central Bank, whose currency is available for settlement-related processing in T2S, or a member of a Central Bank having a contractual relationship with the Central Bank for the processing of its settlement-related cash-processing activities in T2S.</td>
</tr>
<tr>
<td>‘T2S Board’</td>
<td>means the Eurosystem management body established pursuant to Decision ECB/2012/6, which has the task of developing proposals for the Governing Council on key strategic issues and executing tasks of a purely technical nature in relation to T2S.</td>
</tr>
<tr>
<td>‘T2S Business Application’</td>
<td>means the software developed and operated by the 4CB on behalf of the Eurosystem with a view to enabling the Eurosystem to provide the T2S Services on the T2S Platform.</td>
</tr>
<tr>
<td>‘T2S Documentation’</td>
<td>means the T2S non-scope defining set of documents that consists of the other T2S Specification Documents, the T2S Operational Phase Documents and the T2S Project Documents as described in Schedule 2 Annex 8 (T2S Deliverables List and Management Process).</td>
</tr>
<tr>
<td>‘T2S Go-Live Date’</td>
<td>means the first Settlement Day after which the first Participating CSD(s) has/have migrated to T2S.</td>
</tr>
<tr>
<td>‘T2S Memorandum of Understanding’</td>
<td>means the Memorandum of Understanding concluded on 16 July 2009 between the Eurosystem and the Contracting CSD as well as other European CSDs, showing the commitment towards T2S and setting out the mutual obligations and responsibilities for the time frame up to the conclusion of a definitive agreement.</td>
</tr>
<tr>
<td>‘T2S Operator’</td>
<td>means the legal and/or organisational entity/entities that operates/operate the T2S Platform. As part of an internal distribution of work within the Eurosystem, the Governing Council entrusted the 4CB with operating T2S on behalf of the Eurosystem.</td>
</tr>
<tr>
<td>‘T2S Operational Phase Documents’</td>
<td>means the set of documents that describes how T2S provides its services when it is in production. It encompasses the documentation for T2S as a software application and the manuals describing the rules and procedures for operating T2S.</td>
</tr>
<tr>
<td>‘T2S Platform’ or ‘TARGET2-Securities (T2S)’</td>
<td>see ‘TARGET2-Securities (T2S)’.</td>
</tr>
<tr>
<td>‘T2S Programme’</td>
<td>means the set of related activities and deliverables needed to develop T2S until the full migration of all CSDs which have signed this Agreement and all Eurosystem central banks and non-euro area NCBs.</td>
</tr>
<tr>
<td>‘T2S Programme Plan’</td>
<td>means the common Eurosystem-CSD-Central Bank plan, outlining the milestones and timelines to deliver the T2S Programme as well as the actions and contributions required from the Eurosystem, the CSDs and other T2S Stakeholders, as described in Schedule 2 (T2S Programme Planning and Monitoring).</td>
</tr>
</tbody>
</table>
**Schedule 1 – Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘T2S Project Documents’</td>
<td>means the set of documents required for planning, monitoring and successfully completing the scheduled activities (e.g. User Testing, Migration, client readiness tracking) in the T2S project lifecycle but not during the operational part, i.e. from the start of the T2S Programme until T2S is live, or during any subsequent preparation for releases.</td>
</tr>
<tr>
<td>‘T2S Scope Defining Set of Documents’</td>
<td>means the set of documents defining the scope of T2S composed of the URD, the UDFS, the GUI Business Functionality, GFS Functional Chapter, the Data Migration Tool Requirements and Related Procedures and the Data Migration Tool File Specifications.</td>
</tr>
<tr>
<td>‘T2S Services’</td>
<td>means the services to be provided by the Eurosystem to the Contracting CSD as specified in this Agreement.</td>
</tr>
<tr>
<td>‘T2S Stakeholder’</td>
<td>means any organisation, legal entity or governmental entity, public or private interest groups, or individual that has a valid interest in the outcome of the T2S project and the governance and operation of T2S.</td>
</tr>
<tr>
<td>‘T2S Threat Catalogue’</td>
<td>means the information on relevant threats to the T2S Platform, which serves as the basis for the specification of appropriate security controls and, at a later stage, the evaluation of residual risks in terms of impact and likelihood, as described in Schedule 10 (Information Security).</td>
</tr>
<tr>
<td>‘T2S User’ or ‘User’</td>
<td>see ‘User’.</td>
</tr>
<tr>
<td>‘TARGET2-Securities (T2S)’ or ‘T2S Platform’</td>
<td>means the set of hardware, software and other technical infrastructure components through which the Eurosystem provides the services to CSDs that allow core, neutral and borderless settlement of securities transactions on a DvP basis in Central Bank Money.</td>
</tr>
<tr>
<td>‘Technical Disconnection’</td>
<td>means the action motivated by an imminent threat to the security or availability of the T2S Platform, whereby the Eurosystem, in its capacity of operator of T2S, technically blocks the access to the T2S Platform for one or more Directly Connected T2S Actors until such threat has been neutralised.</td>
</tr>
<tr>
<td>‘Technical Issuer CSD’</td>
<td>means a CSD where the security holdings of the participants of an Investor CSD are deposited.</td>
</tr>
<tr>
<td>‘Third Party’</td>
<td>means an individual or legal entity, which is not party to this Agreement. For the avoidance of doubt, a Third Party is a person or legal entity other than the Contracting CSD, the ECB, the euro area NCBs or the T2S Operator.</td>
</tr>
</tbody>
</table>
### Schedule 1 – Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Transactional Data’</td>
<td>means the information that T2S creates and stores through the execution of a business process event, where the content of the information defines that event. This includes but is not limited to inbound and outbound XML messages, all types of settlement instructions and all data that T2S generates for the life cycle of the instruction (e.g. securities positions) and static data maintenance instructions. This is also referred to as Dynamic Data in the Schedules and in other documentation.</td>
</tr>
<tr>
<td>‘Transfer Order’</td>
<td>has the meaning set out in article 2(i) of Directive 98/26/CE.</td>
</tr>
<tr>
<td>‘User Detailed Functional Specifications (UDFS)’</td>
<td>means a detailed description of the functions managing the T2S external data flows (from A2A). It will include the necessary information for the users to adjust or to develop their internal information systems with a view to connecting them to T2S.</td>
</tr>
<tr>
<td>‘User Handbook (UHB)’</td>
<td>means the document describing the way in which T2S Users can make use of a number of T2S software functions that are available in a U2A (screen-based) mode.</td>
</tr>
<tr>
<td>‘User Requirements Document (URD)’</td>
<td>means the document setting out the user requirements for T2S as published by the ECB on 3 July 2008 and as subsequently amended through the T2S change and release management procedure.</td>
</tr>
<tr>
<td>‘User’ or ‘T2S User’</td>
<td>means a CSD participant (a legal entity or, as the case may be, an individual) having a contractual relationship with the CSD for the processing of its securities settlement-related activities in T2S, or a member of a Central Bank (whose currency is available for settlement-related processing in T2S) having a contractual relationship with the Central Bank for the processing of its securities settlement-related cash-processing activities in T2S.</td>
</tr>
<tr>
<td>‘User Testing’ or ‘User Tests’</td>
<td>means a set of rules and procedures concerning the testing of T2S by CSDs as described in Schedule 3 (User Testing).</td>
</tr>
<tr>
<td>‘User-to-Application (‘U2A’)’</td>
<td>means a connectivity mode to exchange information between software applications of T2S and a T2S Actor through a GUI.</td>
</tr>
<tr>
<td>‘Value-added Connection’</td>
<td>means a solution to connect the T2S data centres with the data centres of the Directly Connected T2S Actors, whereby both the Value-added Connectivity Services and the Physical Connectivity Services are provided by a NSP.</td>
</tr>
<tr>
<td>‘Value-added Connectivity Services’</td>
<td>means the set of messaging services, security services and operational services either provided by a NSP in accordance with the Licence Agreement, or implemented in T2S and in the systems of the Directly Connected T2S Actors.</td>
</tr>
</tbody>
</table>
Annex 1 – Diagram of Phases / Periods

- **Start of Migration Activities (SP14)**
- **Wave I Migration Weekend**
- **Contingency Wave Migration & Go-Live**
- **Closing T2S Programme (SP 17)**

---

**Migration Period**

**User Testing Execution Phase**

**Development Phase**

**Operational Phase**

**T2S Go-Live Date**
FRAMEWORK AGREEMENT

SCHEDULE 2

T2S PROGRAMME PLANNING AND MONITORING
# Framework Agreement

## Schedule 2 – T2S Programme Planning and Monitoring

### Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>INTRODUCTION</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Context</td>
<td>1</td>
</tr>
<tr>
<td>1.2</td>
<td>Structure of Schedule</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>SCOPE AND OBJECTIVES</td>
<td>4</td>
</tr>
<tr>
<td>2.1</td>
<td>Scope</td>
<td>4</td>
</tr>
<tr>
<td>2.2</td>
<td>Objectives</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>GENERAL RESPONSIBILITIES OF THE PARTIES TO THIS AGREEMENT</td>
<td>5</td>
</tr>
<tr>
<td>3.1</td>
<td>General Responsibilities of the Eurosystem</td>
<td>5</td>
</tr>
<tr>
<td>3.2</td>
<td>General Responsibilities of the Contracting National Central Banks (CBs)</td>
<td>5</td>
</tr>
<tr>
<td>3.3</td>
<td>General responsibilities of the Project Manager Group (PMG)</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>SUPPORTING DOCUMENTATION</td>
<td>8</td>
</tr>
<tr>
<td>4.1</td>
<td>T2S Programme Work Breakdown Structure</td>
<td>8</td>
</tr>
<tr>
<td>4.2</td>
<td>T2S Programme Deliverables</td>
<td>8</td>
</tr>
<tr>
<td>4.3</td>
<td>Milestones</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>T2S PROGRAMME PLAN</td>
<td>10</td>
</tr>
<tr>
<td>5.1</td>
<td>CB-relevance of planning items</td>
<td>10</td>
</tr>
<tr>
<td>5.2</td>
<td>T2S Programme Plan Views</td>
<td>11</td>
</tr>
<tr>
<td>5.3</td>
<td>T2S Critical Path</td>
<td>14</td>
</tr>
<tr>
<td>6</td>
<td>MONITORING FRAMEWORKS</td>
<td>15</td>
</tr>
<tr>
<td>6.1</td>
<td>T2S Programme Status Assessment Framework</td>
<td>15</td>
</tr>
<tr>
<td>6.2</td>
<td>T2S Risk and Issue Management and Monitoring Framework</td>
<td>17</td>
</tr>
<tr>
<td>6.3</td>
<td>T2S Monitoring of Client Readiness Framework</td>
<td>22</td>
</tr>
<tr>
<td>7</td>
<td>PROCESSES</td>
<td>27</td>
</tr>
<tr>
<td>7.1</td>
<td>Methodology and Conventions</td>
<td>27</td>
</tr>
<tr>
<td>7.2</td>
<td>Programme Plan Preparation, Adaptation and Assessment Review Process</td>
<td>29</td>
</tr>
<tr>
<td>7.3</td>
<td>Adaptation Process for updated Annexes without affecting the plan</td>
<td>32</td>
</tr>
<tr>
<td>7.4</td>
<td>Disagreement Resolution process</td>
<td>34</td>
</tr>
</tbody>
</table>

19 March 2014
1 Introduction

1.1 Context

T2S is a large-scale programme, involving a significant number of actors. Owing to this complexity, a successful development, implementation and production start of T2S requires agreement between the parties to this Agreement on their roles and responsibilities as well as the respective expectations and commitments during the programme. It is not sufficient for the parties to this Agreement to the T2S Programme to establish and monitor stand-alone project plans independently of each other. It requires a common programme plan that:

- is based upon clearly identified and scoped deliverables;
- takes into account all the respective constraints and dependencies of the parties to this Agreement; and
- undergoes regular, close monitoring over the life of the programme, with decisions committing all parties.

As the plan may evolve during the course of the T2S Programme, a comprehensive framework must exist to manage events that may affect the programme’s deliverables and milestones, including a review and decision-making process for adapting the programme plan. This requires a regular dialogue between the parties to this Agreement to enable them to manage their own parts of the programme, and jointly make proposals on common tasks and activities affecting the other parties to this Agreement. Contracting Central Securities Depositories (CSDs) must be in the position to organise their planning and their internal resources. Conversely, the Eurosystem planning of the User Testing and Migration phases, as well as the start operations in T2S, requires the input of all T2S Actors.

A successful programme delivery requires a consistent and complete framework to plan, coordinate, monitor and report the activities of the T2S Actors. Article 25 of the FA defines the process of updating this Schedule 2. This Schedule 2 specifies the process of updating the Annexes of Schedule 2 (see Section 7).
1.2 Structure of Schedule

The Schedule 2 contains different sections and has several Annexes.

The second section presents the scope and objectives of Schedule 2.

The third section presents the general responsibilities of the Eurosystem and the Contracting CSDs.

The fourth section describes the main documents supporting the monitoring of the T2S Programme Plan.

The fifth section presents the three official views of the T2S Programme plan and their main features.

The sixth section presents the main principles and conventions used for progress monitoring, for risk monitoring and for the management of bilateral relations between the Eurosystem and each Contracting CSD.

The seventh section documents the T2S Programme Plan monitoring process and includes the process for changing Schedule 2 Annexes.

The Annexes to Schedule 2 have three objectives:

- to provide the initial state of the T2S Programme planning documentation, which may evolve according to the processes defined in Schedule 2;
- to provide the templates used for programme reporting purposes; and
- to provide the initial state of the supporting documentation.

Schedule 2 includes the following Annexes:

Annexes with focus on the plan substance:
- Annex 1 - T2S Executive Summary Plan
- Annex 2 - T2S Operational Plan
- Annex 3 - T2S Detailed Plan
- Annex 4 - T2S Programme Plan assumptions

Annexes with focus on reporting templates:
Framework Agreement
Schedule 2 – T2S Programme Planning and Monitoring

54  ▪  Annex 5 - T2S Programme Progress Reporting templates

55  ▪  Annex 6 - T2S Risk and Issue Reporting templates

56  Annexes with focus on supporting documents:

57  ▪  Annex 7 - T2S Programme Work Breakdown Structure (WBS)

58  ▪  Annex 8 - T2S list of Deliverables

59  ▪  Annex 9 - T2S list of Synchronisation points

60  ▪  Annex 10 - T2S list of Milestones on the critical path
2 Scope and Objectives

2.1 Scope
This document on Programme Planning and Monitoring (Schedule 2 of the FA) presents the commitment of the Eurosystem to establish and maintain a common programme plan (the T2S Programme Plan) and defines the roles, responsibilities, processes and interactions of the parties to this Agreement.

2.2 Objectives
The objectives of Schedule 2 are:

- to document the baseline T2S Programme Plan and its underlying assumptions;
- to define the framework for coordinating, managing and attempting to resolve potential disagreement on the T2S Programme Plan;
- to provide all parties to this Agreement with the necessary information to develop, coordinate and manage their respective project plans in coordination with the T2S Programme Plan;
- to define a monitoring and reporting framework on the progress against the T2S Programme Plan, including risks and issues; and
- to define a monitoring framework for client readiness.
3 General Responsibilities of the parties to this Agreement

3.1 General Responsibilities of the Eurosystem

The Eurosystem commits to deliver and maintain the documentation, frameworks and processes, as defined in this Schedule and its Annexes. This means that at any point in time there will be a valid programme plan and an agreed framework to provide all parties to this Agreement with relevant information on the programme status detailing the main principles, frameworks, processes and tools to support the programme monitoring. The Eurosystem commits to follow the framework and processes defined in this Schedule.

Furthermore, the responsibilities of the Eurosystem include:

- preparing and maintaining the T2S Programme Plan;
- organizing a close coordination with Contracting CSDs for reviewing and proposing changes to the plan to the Steering Level;
- providing on a regular basis to Contracting CSDs an accurate T2S Programme status assessment based on the T2S Programme Plan;
- preparing reports on, and response plans for, risks and issues pertaining to the T2S Programme Plan with emphasis on activities and deliverables that impact Contracting CSDs;
- establishing and chairing the Project Managers Group (PMG) to review, discuss and agree on the T2S Operational Plan and the T2S Programme status for Contracting CSDs relevant planning items with Contracting CSDs and Contracting CBs; and
- establishing and attending a bilateral forum between the Eurosystem and each Contracting CSD to review and discuss the Contracting CSD’s individual status assessment for their activities within the T2S Programme Plan.

3.2 General Responsibilities of the Contracting Central Securities Depositories (CSDs)

Contracting CSDs are responsible for ensuring their own readiness and for undertaking reasonable efforts to coordinate the readiness of their clients (including those who are directly connected to T2S) to start with T2S. Contracting CSDs commit to follow the framework and processes defined in this Schedule and its Annexes.
Furthermore, the responsibilities of the Contracting CSDs include:

- establishing their own adaptation plans to start operations with T2S in synchronisation with the T2S Programme Plan;
- providing relevant and accurate information on progress and achievement of milestones, deliverables and synchronisation points, as well as on risks and issues, including response plans, potentially affecting the T2S Programme Plan. This is to enable the Eurosystem to maintain the T2S Programme Plan and consolidate the information received in the context of the monitoring of client readiness;
- participating in the PMG to review, discuss and agree on the T2S Operational Plan and the T2S Programme status for activities, deliverables and milestones affecting the plans of Contracting CSDs; and
- participating in a bilateral forum between the Eurosystsem and each Contracting CSD to review and discuss the Contracting CSD’s individual status assessment of its activities within the T2S Programme Plan to become operational on T2S.
3.3 General responsibilities of the Project Manager Group (PMG)

The PMG shall be composed of representatives of the Eurosystem, Contracting CSDs and Contracting CBs. Schedule 1 and Schedule 8 define the general role of the PMG. The following specifies the responsibilities of the PMG when supporting activities as defined in Schedule 2. The PMG shall:

- Meet (physically or via conference call) on a regular basis and on an ad hoc basis when requested by one of the members. The PMG determines the frequency of its meetings based on its needs.
- Assess the T2S Operational Plan and propose updates as detailed in Section 7.
- Assess the T2S Programme status report and propose changes.
- Identify risks and issues related to the execution of the T2S Plan.
- Propose mitigation or resolution measures for all risks and issues identified.
- Discuss and propose solutions for multilateral issues related to the readiness of one of its members.
- Act proactively and in good faith to achieve agreement between PMG members.
- Prepare escalations on and escalate disagreements to the Steering Level.
- Be informed on a regular (e.g. quarterly) basis and identify the needs of the changes to the T2S Scope Defining Set of Documents.
4 Supporting Documentation

The Eurosystem provides the documents described in this section as background information supporting programme planning and monitoring. The Annexes to Schedule 2 contain the baseline versions of these documents. These documents may evolve in the course of the programme as defined by the processes in Section 7.

The supporting documentation provides the reference that allows the reader to understand the content and construction of the plans and reports.

4.1 T2S Programme Work Breakdown Structure

The Eurosystem defines and maintains a Work Breakdown Structure (WBS) for the purpose of programme planning and monitoring. The WBS is a Deliverable-oriented hierarchical decomposition of the work that the T2S Programme needs to execute to deliver T2S successfully. The WBS is the basis for grouping, aggregating and classifying the activities and deliverables for the T2S Programme Plan as well as for T2S programme status monitoring.

4.2 T2S Programme Deliverables

A Deliverable is a unique and verifiable product, result, or capabilities to perform a service, required to complete a process or phase\(^1\).

The specification of the Deliverable consists of the information documented in the introduction to Annex 8 (e.g. name of the Deliverable, its classification according to the WBS)

The Eurosystem defines and maintains the List of Deliverables.

---

\(^1\) In line with the PMBOK®

19 March 2014  Page 8 of 36
4.3 Milestones

Milestones are significant points or events in the programme\(^2\). In addition to this standard milestone definition, the T2S Programme Plan includes specific milestones as defined in the subsequent paragraphs.

4.3.1 Synchronisation Points

A synchronisation point is a point of time in the programme at which the T2S Programme is to reach a specific objective. The purpose of a synchronisation point is to monitor at foreseen time intervals that the progress of all parties to this Agreement is in line with the programme plan.

The Eurosystem provides the list of synchronisation points, which includes the list of the deliverables and milestones that require delivery or completion by the Eurosystem, Contracting CSDs and Contracting CBs in order to have successfully achieved the synchronisation point.

4.3.2 Critical Milestones

Critical milestones are milestones on the critical path of the T2S Programme Plan. Please refer to Section 5.3 for the definition of the T2S Critical Path.

4.3.3 Key Milestones

Key milestones are specific Synchronisation Points, which, in case of delay, might trigger legal/financial consequences as defined in the FA Article 31. Therefore, any update of the Key Milestones’ dates follows the FA updating process.

\(^2\) In line with the PMBOK\(^\text{®}\)
5 T2S Programme Plan

The T2S Programme Plan is the common Eurosystem-CSD-CB plan. This chapter describes the three views of the T2S Programme Plan that the Eurosystem provides in order to allow Contracting CSDs and Contracting CBs to monitor the progress of the T2S Programme and update their own plans.

The T2S Programme WBS, based on work streams, provides the organisational structure for activities, tasks, and milestones of the plans.

5.1 CSD-relevance of planning items

The T2S Programme Plan differentiates between CSD-relevant, non-CSD-relevant and CSD-internal planning items, specifically identified in the T2S Programme Plan.

5.1.1 CSD-relevant planning items

These are planning items (e.g. deliverables, milestones and processes) affecting, or being affected by, the Contracting CSDs.

- Deliverables are CSD-relevant if the Contracting CSD is:
  - the assignee;
  - the addressee;
  - the reviewer; or
  - being consulted.

- Meetings, workshops are CSD-relevant when:
  - the Contracting CSD is participating (e.g. CSG, PMG, AG, Sub Groups); or
  - feedback is expected on specific topics (e.g. planning workshops).

- Programme phases, activities and tasks are CSD-relevant when the Contracting CSD is involved as an actor, e.g. as a reviewer or an observer.

- Programme phases, activities and tasks affecting the successful and timely completion of the Synchronisation Points.
The Eurosystem will provide status reporting on these items in the PMG. Contracting CSDs can review/analyse, discuss, and envisage alternative solutions for these items.

### 5.1.2 Non CSD–relevant planning items

These are planning items (e.g. deliverables, milestones and processes) that do not require any Contracting CSD involvement. The T2S Programme Plan does not present the details of activities or steps leading to a deliverable, but it provides milestones and summary tasks to ease plan readability.

Some examples for these items:

- Internal Eurosystem activities or deliverables not impacting the critical path or the delivery of a Contracting CSD deliverable (e.g. Internal Detailed Functional Specifications, Internal development process);
- predecessors of the processes highlighted above (all the tasks preparatory to the deliverables, e.g. information security preparatory work related to the deliverable ‘risk assessment’); and
- independent processes (e.g. Internal Eurosystem governance).

The Eurosystem shall provide status reporting and information on planning items that are not CSD-relevant that are in the Operational Plan. However, Contracting CSDs do not analyse and propose alternative solutions for these planning items.

### 5.1.3 Internal CSD planning items

The T2S Programme Plan presents the main dependencies, relating to the completion process for specific milestones, called *Synchronisation Points*. Since Contracting CSDs may be ready at various points in time, the T2S Programme Plan only presents the ultimate deadline before a delay could affect the critical path.

In the context of the monitoring of client readiness, Contracting CSDs report progress on these items to their relationship manager, who in turn reports to the PMG. These items are under management responsibility of the Contracting CSD. Therefore, the Eurosystem does not analyse or propose alternative solutions for these items.

### 5.2 T2S Programme Plan Views

The Eurosystem ensures the synchronisation of three different views of the T2S Programme Plan:
Framework Agreement
Schedule 2 – T2S Programme Planning and Monitoring

- the T2S Detailed Plan, which presents the most detailed level and is to be used as reference to support detailed discussions when issues arise at the level of the T2S Operational Plan;
- the T2S Operational Plan, which forms the baseline subject to monitoring at PMG level;
- the T2S Executive Summary Plan, which is the plan communicated externally and which contains the most important dates of the T2S Programme Plan.

The Eurosystem produces an initial version of the plans in June of each year. The Eurosystem reviews the draft plans with Contracting CSDs, wherever CSD-relevant, in order to deliver an agreed T2S Operational Plan in September following the process described in Section 7 of the present Schedule.

5.2.1 T2S Detailed Plan

The T2S Detailed Plan provides for the T2S Programme the accurate and detailed planning for all deliverables and activities, relevant for Contracting CSDs as well as selected deliverables, milestones and activities not CSD-relevant or CSD-internal to ease readability. It also provides the necessary details until the end of the project, bearing in mind that the accuracy of the information decrease with time. The purpose of the T2S Detailed Plan is to provide the single point of reference and to support discussion within the PMG when the T2S Operational Plan does not provide sufficient detail.

The Eurosystem produces an updated version of this plan in June. The Eurosystem reviews a draft T2S Detailed Plan with Contracting CSDs, wherever CSD-relevant, to support the delivery of the T2S Operational Plan in September.

The T2S Detailed Plan specifies:

- all CSD-relevant deliverables, milestones and activities (flagged as “CSD-relevant”);
- selected deliverables, milestones and tasks that are not-CSD-relevant or CSD-internal, but required for the understanding of the plan and for a global overview of the programme;
- the synchronisation points for the monitoring of client readiness for Contracting CSDs and Contracting CBs; and
- a Schedule of meetings and workshops, requiring the participation of Contracting CSDs and/or Contracting CBs.
The T2S Programme Office provides updates of this plan as references to support the bilateral meetings for monitoring of client readiness (MCR) and the meetings of the PMG.

Should a regular update relate to an internal Eurosystem activity (4CB or ECB) and have no impact on the T2S Operational Plan (e.g. critical path, readiness; review period, etc.), the Eurosystem amends the T2S Detailed Plan, without prior discussion at PMG level.

5.2.2 T2S Operational Plan (One-Year Rolling)

The T2S Operational Plan aggregates the detail of the T2S Detailed Plan for one calendar year, including all tasks starting and/or finishing in that year. It also provides summary tasks and activities for the subsequent years until completion of the programme. This plan forms the baseline and is the basis for the reporting of the T2S Programme status. The purpose of the T2S Operational plan is:

- to coordinate the activities and interactions on deliverables between the Eurosystem and Contracting CSDs;
- to enable Contracting CSDs to develop and to monitor their own internal plans for T2S and to determine their resource requirements; and
- to support Contracting CSDs in performing their own assessment of the progress of the T2S Programme.

The T2S Operational Plan specifies for the one calendar year:

- all major deliverables, dependencies, milestones and aggregated tasks;
- whether a planning item is CSD-relevant;
- the synchronisation point for the monitoring of client readiness for Contracting CSDs and Contracting CBs; and
- a summary task of the period of time requiring the participation of Contracting CSDs and/or Contracting CBs.
The Eurosystem provides updates of this plan to support the meetings for monitoring of client readiness and the meetings of the PMG. If a planning update affects another party (in the larger sense: readiness with external provider, review period, dependency Eurosystem, Contracting CSDs and Contracting CBs etc…) or influences the critical path, focussed information will be provided, including the explanation of the issue, the impact analysis and whenever relevant, the presentation of alternative solutions to be envisaged.

5.2.3 T2S Executive Summary Plan

The T2S Executive Summary Plan documents the milestones, synchronisation points and the duration of activities for the major deliverables and phases of the T2S Programme in order to provide a high-level summary view of the T2S Programme Plan.

5.3 T2S Critical Path

The critical path is the sequence of activities/tasks with the longest overall duration, determining the shortest time possible to complete the programme.

The T2S Detailed Plan documents the critical path for the Eurosystem activities and includes some external dependencies such as activities of Contracting CSDs. Building the critical path for external dependencies requires a series of assumptions, as the plan cannot reflect detailed dependencies with each Contracting CSD. The Eurosystem provides all such assumptions (Annex 4 to this Schedule) when providing the T2S Detailed Plan. The T2S Detailed and T2S Operational Plan highlights (MS Project) the tasks belonging at the critical path in red. The critical path may change because of updates of the T2S Detailed Plan.
6 Monitoring frameworks

The next sections define supporting materials and the methodology followed to assess progress and report the risks and issues. Section 7 describes the underlying process.

6.1 T2S Programme Status Assessment Framework

6.1.1 Objectives and Scope

The Eurosystem establishes a T2S Programme status assessment framework. The objectives of the framework are:

- Organise regular reporting to all parties to this Agreement at the various levels of governance about the progress of the T2S Programme against the T2S Operational Plan;
- to enable proper monitoring by providing a status report;
- to facilitate the coordination of activities and interactions on deliverables between the Eurosystem and the Contracting CSDs; and
- to ensure that possible plan deviations against the Operational Plan are identified, discussed and addressed in a timely and appropriate manner.

In regularly scheduled (multilateral) assessment meetings with Contracting CSDs, the Eurosystem reports on the progress against the T2S Operational Plan. Contracting CSDs report their progress on deliverables pertaining to synchronisation points on a bilateral basis as part of the monitoring of client readiness.

6.1.2 Key Element of Programme Status Assessment and Monitoring

The process description for programme assessment and monitoring is Annex 5 to this Schedule.
6.1.2.1 T2S Progress Dashboard

The T2S Programme WBS specifies the structure of the dashboard template, presented in Annex 5 and 6 to this Schedule. Using the WBS, the T2S dashboard presents a high-level overview of the progress achieved and the overall risk situation for the main streams of the programme (aggregation of activities and deliverables at work stream level).

The T2S Progress Dashboard presents the following elements:

- status, with colour coding;
- change (for status), compared to previous report;
- trend, expected in the next report;
- risk, with colour coding; and
- change, (for risk) compared to previous report.

6.1.2.2 T2S Programme Status Report

The Eurosystem provides a T2S Programme Status. The T2S Programme Status Report includes:

- the high-level T2S Progress Dashboard, as described in the previous Section;
- per work stream a status assessment for each CSD-relevant deliverable with a status “green”, “yellow” or “red”;
- per work stream a detailed status assessment for each CSD-relevant deliverable with a status “yellow” or “red”;
- per work stream a risk assessment for each CSD-relevant deliverable. A detailed risk assessment is provided in case the risk criticality is “yellow” or “red”; and
- per work stream an issue description (incl. a response plan) for each issue pertaining to a CSD-relevant Deliverable, in case a risk has materialised.

6.1.2.3 Conventions

The Eurosystem prepares a programme status assessment for each Deliverable, using colour coding (Green/Yellow/Red). This assessment evaluates the status of a Deliverable based on time, quality and scope.
A specific colour, based on a three colours scheme, specifies the progress:

<table>
<thead>
<tr>
<th>Colour</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>Deliverable is within the required scope and quality and is on time</td>
</tr>
<tr>
<td>Yellow</td>
<td>Deliverable will not have the required scope, will be delayed and/or not of the required quality if no corrective measures are taken</td>
</tr>
<tr>
<td>Red</td>
<td>Corrective measures have not delivered the expected effect or no corrective measures are possible. Deliverable will be delayed to achieve the required quality or scope if no extraordinary action is taken and requires escalation as described in section 7.2.</td>
</tr>
</tbody>
</table>

In addition to the colour reported for the progress assessment, the reporting of the Deliverable shows:

- the change from the previous progress assessment; and
- the expected trend for the next monitoring period.

The T2S Programme Status Report provides detailed information for each activity or Deliverable with a “yellow” or “red” status, including:

- the list of achievements;
- when relevant, the list of milestones missed or delayed; and
- the list of mitigating actions already started or envisaged to manage the situation.

### 6.2 T2S Risk and Issue Management and Monitoring Framework

#### 6.2.1 Definitions, Scope and Objectives

The Eurosystem establishes a T2S Risk and Issue Management and Reporting Framework as a comprehensive tool for the handling of risks and issues. The term ‘risk’ refers to a ‘threat’ to the successful delivery of the T2S Programme. The framework does not track and manage ‘opportunities’. ‘Issues’ define materialised risks.

The objectives of the framework that all parties to this Agreement are to follow are:

- to identify, manage and monitor risks and issues, potentially affecting the successful delivery of the T2S Programme;
- to inform and discuss between all parties to this Agreement in case of risks/issues, which may
 Framework Agreement
Schedule 2 – T2S Programme Planning and Monitoring

6.2.2 Principles

The T2S Risk and Issue Management and Reporting Framework covers all risks, which may materialise during the programme’s lifetime (i.e. from today until ‘start operation’) and all identified issues. The framework also foresees for each risk a root cause analysis, which identifies the underlying cause leading to the risk. The assumption is that one root cause will exist for each risk.

The assessment of programme risks applies a common grading scale for probability and impact. A probability/impact matrix is then applied to determine the criticality zone each risk is allocated to. The actual risk situation (reflecting the status of implementation of mitigation measures) is decisive for assessing the criticality.

The parties to this Agreement shall report:

- risks and the related risk response strategy as soon as possible following the formal risk assessment; and
- issues as soon as possible after their identification.

6.2.3 Risk and Issue Identification and Registration

All parties to this Agreement ensure that the appropriate risk and issue management functions as well as operational processes are in place for the registration of identified risks and issues, potentially affecting the various programme deliverables and milestones. All parties to this Agreement commit to share risks and issues in the appropriate forums, as defined hereafter in the Sections “T2S Monitoring of Client Readiness Framework” and “Processes”.

6.2.4 Risk Assessment

The party to this Agreement identifying a risk (risk owner) shall evaluate the risk, based on:

- the impact on the T2S Programme; and
the probability of the risk materialising.

6.2.4.1 Risk Impact Grading Scale

The T2S Risk and Issue Management Framework applies a five-level impact grading scale:

<table>
<thead>
<tr>
<th>Impact Level</th>
<th>5 Very Severe</th>
<th>4 Major</th>
<th>3 Significant</th>
<th>2 Low</th>
<th>1 Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Objective</td>
<td>Project end item is effectively useless</td>
<td>Scope change unacceptable</td>
<td>Major areas of scope affected</td>
<td>Minor areas of scope affected</td>
<td>Scope impact barely noticeable</td>
</tr>
<tr>
<td>Quality</td>
<td>Project end item is effectively useless</td>
<td>Quality reduction unacceptable</td>
<td>Quality reduction requires an approval</td>
<td>Only very demanding applications are affected</td>
<td>Quality degradation barely noticeable</td>
</tr>
<tr>
<td>Cost</td>
<td>&gt; 10 M euros</td>
<td>1M – 10M euros</td>
<td>100,000 – 1M euros</td>
<td>10,000 – 100,000 euros</td>
<td>&lt;10,000 euros</td>
</tr>
<tr>
<td>Time³</td>
<td>&gt; 20% time increase</td>
<td>10 - 20% time increase</td>
<td>5 - 10% time increase</td>
<td>1 - 5% time increase</td>
<td>&lt; 1% time increase</td>
</tr>
</tbody>
</table>

Figure 1: Risk Impact Grading Scale

The programme objectives scope, quality, cost and time are the basis for evaluating the risk impact, following the international standard Project Management Book of Knowledge (PMBOK) with the exception of the cost dimension. The use of this standard facilitates the assessment of the risk by determining the effect of the materialisation of an identified risk on each project objective. The highest category of the risk’s impact on a project objective defines the overall impact of the risk.

³ The percentages are calculated against the overall project duration.
6.2.4.2 Risk Probability Grading Scale

The T2S Risk and Issue Management Framework applies a five-level probability grading scale.

<table>
<thead>
<tr>
<th>Risk Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>Very Unlikely</td>
</tr>
</tbody>
</table>

Figure 2: Risk Probability Grading Scale

The description of the risk probability level uses a percentage to classify the risk according to a probability that it materialises. When possible, the assessment of the probability of a risk eventuating is based on comparable large-scale programmes. However, the experience of management in similar programmes and projects and the experience in operating in similar complex environments and organisations are also factors in determining the probability for common risk programme risks.

6.2.4.3 Probability-Impact Matrix

The impact of a T2S-related risk and the probability of occurring determine its level of criticality. The T2S Programme uses the following probability/impact matrix for determining the criticality of a risk according to a three colour scheme.

<table>
<thead>
<tr>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Red</td>
</tr>
<tr>
<td>4 Yellow</td>
</tr>
<tr>
<td>3 Green</td>
</tr>
<tr>
<td>2 Green</td>
</tr>
<tr>
<td>1 Green</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

Figure 3: Probability-Impact Matrix

- The intersection between the impact of the risk and its probability in the matrix specifies the level of criticality of a risk to the T2S Programme (labelled with the colours green, yellow and red). The level of criticality determines on how the risk is managed.
In case the criticality level of a work stream for which several risks have been identified needs to be determined, the most severe risk determines the criticality level of the entire work stream.

6.2.5 Risk Tolerance Policy

The T2S Programme risk tolerance policy defines the level of programme risk that the ECB (ESCB/Eurosystem) is prepared to accept. The T2S Programme risk tolerance policy stipulates that the criticality of a risk and determines the body responsible for accepting a non-mitigated risk. The framework considers risks allocated to the green criticality level as accepted ex ante. All risks allocated beyond the tolerated level, i.e. those in the yellow and red zone, are subject to further risk management measures. Risks allocated to the red zone have the highest priority for mitigation.

6.2.6 Risk Response Plan

Risk response plans address identified T2S risks. Unless exempted by the confidentiality rules, the PMG monitors the implementation of the risk response plan, as indicated in the risk identification form, based on status reports received from the risk owners. The T2S Programme Office informs the Steering Level of the status of mitigation via the regular status reports. In case the risk has been reported to the other parties to this Agreement, the respective status information is provided in the (multilateral) monitoring meetings as defined hereafter in the Sections “T2S Monitoring of Client Readiness Framework” and “Processes”.

6.2.7 Issue Response Plan

Issue Response Plans address identified issues affecting the successfully delivery of T2S. The implementation of the issue response plan and sharing of information on issues is analogous to the process for risk response plans.

6.2.8 Risk/Issue Reporting

Based on the information received via the risk/issue notification forms, the Eurosystem registers each identified risk/issue. A risk/issue sheet provides high-level information on the risk/issue and its background and forms part of the T2S Programme Status Report.
6.3 T2S Monitoring of Client Readiness Framework

6.3.1 Definitions, Objectives and Scope

In the context of this Schedule, Client Readiness is defined as the capability of a Contracting CSD (and their respective communities - including DCP) to fulfil the legal, functional, technical and organisational requirements (i.e. all showstopper are resolved) to start operation in T2S relative to the synchronisation points (CSD-relevant milestones), as specified in the T2S Programme Plan.

The term Monitoring of Client Readiness (MCR) defines the framework to ascertain the readiness of a Contracting CSD (and their respective communities- including DCP) to start operation in T2S based on the Contracting CSDs’ progress against the agreed milestones and deliverables of the T2S Operational Plan for the current phase of the T2S Programme. As a component of T2S Programme Planning and Monitoring, the parties to this Agreement agree to establish such a framework to allow the Eurosystem to monitor the readiness status of Contracting CSDs to start operation with T2S.

The objectives of the MCR Framework are:

- to ensure accurate reporting on the progress of a Contracting CSD regarding its readiness level relative to the T2S Programme Plan;
- to establish the necessary collaborative measures, rules, procedures and tools to support the monitoring process; and
- to foster the communication between individual Contracting CSDs and the Eurosystem on programme-plan-related issues, with a view to ensure timely and proactive identification and notification of any event that would have a material effect on the T2S Programme Plan and the start operation of T2S.

The scope of the MCR includes activities that the Contracting CSDs and their communities (including DCP) must undertake to ensure the required readiness level relative to the T2S Operational Plan and to the successful and timely completion of the Synchronisation Points.
MCR covers all phases of the T2S Programme until start of full operation of T2S with the successful implementation of the last of the planned migration waves. It also includes the monitoring of and reporting on the readiness of the Contracting CSD clients, indirectly and directly connected to T2S. It should be noted that the Contracting CSDs are responsible for tracking their own community (including DCP) and accurately reporting to the Eurosystem.

MCR encompasses the following activities:

- the monitoring of the fulfilment of the mutual obligations, milestones and deliverables;
- the monitoring and review of the mutual obligations in regular intervals and for individual periods, as bilaterally agreed, to ascertain their status as compared to the T2S Programme Plan; and
- the identification and notification of delays or any event affecting the successful and timely completion of the Synchronisation Points.

### 6.3.2 Monitoring of Client Readiness and Reporting

#### 6.3.2.1 Principles

Gathering client readiness relevant information from the Contracting CSD and comparing the Contracting CSD’s adaptation and migration plan to the overall T2S Programme Plan ensures that all Contracting CSDs consistently and jointly progress towards a successful start operation in T2S. At the synchronisation points, the parties to this Agreement can assess whether they remain aligned with the T2S Programme Plan. MCR identifies risks (incl. potential mitigation measures) as well as issues (incl. response plans), which potentially affect the Eurosystem, Contracting CSDs or Contracting CBs or the successful start operation of T2S. Between synchronisation points, the Contracting CSDs and the Eurosystem collaborate closely to support each other in the timely achievement of the relevant assessments, deliverables and milestones.

The parties to this Agreement agree to meet bilaterally to review, assess and discuss the Contracting CSD’s progress at least once per synchronisation point, based on agreed assessment criteria and status reporting methodology of this Schedule. Contracting CSDs agree to report for readiness monitoring:

- the progress against their adaptation plan and status of their deliverables; and
- their risks and issues pertaining to their adaptation and affecting the successful completion of
Framework Agreement
Schedule 2 – T2S Programme Planning and Monitoring

6.3.2.2 Periodicity

The periodicity of meetings is dependent on the phase of the T2S Programme. Meetings will occur:

- on a quarterly basis from the signature of the FA until the start of the User Testing;
- on a monthly basis from the start of User Testing; and
- on an ad hoc basis when requested by one of the parties to this Agreement.

6.3.2.3 Organisation

MCR includes all Contracting CSDs participating in the T2S Programme. The Eurosystem monitors actively the degree of client readiness and asks the Contracting CSDs for regular monitoring of the status of the different activities and of the preparedness level of their communities (including DCP).

The Eurosystem monitors Client Readiness at three levels:

- The first level of monitoring is at the operational level of the client relationship management, with support provided by the other functions of the T2S Programme. The formal communication and exchange of information between the Contracting CSD and the T2S Programme Office takes place by means of (a) written submissions or (b) bilateral meetings between representatives of the Contracting CSD and representatives of the T2S Programme. Aiming at ensuring an efficient and effective communication, a Contracting CSD has a single person of contact within the client relationship area of the T2S Programme. The role of the single person of contact is to bundle the issues, comments and questions of the Contracting CSD, to coordinate and align these issues, comments and questions with other Contracting CSDs and Contracting CBs and to ensure final response and implementation;

- The second level of monitoring of client readiness is at the level of the PMG, which looks for common alternatives to resolve issues causing a delay or a risk of delay to a synchronisation point; and

- The third level of client readiness monitoring is at the Steering Level.
6.3.3 Client Readiness Reporting

The Eurosystem regularly reports on the overall Client Readiness (Contracting CSDs and Contracting CBs) as part of the programme status assessment and discusses the status with the Contracting CSDs in multilateral meetings. The status of a specific Contracting CSD in the context of MCR is subject to the confidentiality and transparency rules (see Section 6.3.4). The Eurosystem intends to publish aggregated client readiness-relevant information on a regular basis to provide a summary of the T2S readiness status covering the entire community (including DCP). The Eurosystem reviews this assessment with the Contracting CSDs prior to publication.

6.3.4 Confidentiality and Transparency Rules

The Eurosystem is committed to full transparency regarding T2S. T2S communication on client readiness addresses a wide spectrum of recipients, comprising individual Contracting CSDs, various T2S governance bodies and the public.

Full transparency does not preclude confidentiality. As a matter of principle, and as reflected in the business rules below, Contracting CSD readiness status and internal issues, discussed in the MCR bilateral meetings, remain confidential unless they affect the overall readiness, other Contracting CSDs, the T2S Programme organisation and/or the T2S business case. Communication of any other topics to a third party shall require prior written mutual consent. The business rules, which govern the confidentiality versus transparency dimensions, are set out below:
Information Exchange → Information Assessment

CSD/CB internal only

No impact
Impact on plan

Confidential with CSD/CB
Depending on impact: PMG/AG

CSD/CB + its community

No impact
Impact on plan

Confidential with CSD/CB/NUG
Depending on impact: PMG/NUG/AG

Other CSDs or CBs

No impact
Impact on plan

Confidential with PMG
Depending on impact: PMG/AG

Other CSDs/CBs + communities

No impact
Impact on plan

Confidential with PMG/NUGs
Depending on impact: PMG/NUG/AG


7 Processes

The below processes only cover topics related to Schedule 2; therefore, the process actors’ roles, as described below, are only applicable to the Schedule 2 topics and should not be read as a limitation to their roles in other topics of the FA.

7.1 Methodology and Conventions

The T2S monitoring process is represented in a diagram and supported by a high–level process description.

Individual sub-processes are described, but not supported by business diagrams.

There is no specific section to describe the individual activities, decision points or business rules.

Likewise, the adaptation process for Schedule 2 Annexes is represented in a diagram and supported by a high-level process description.
### 7.1.1 Standards

This document uses a simplified version of the Business Process Modelling Notation (BPMN) 2.0 notation, as documented below.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Process Name&gt;</td>
<td>Pools (Participants) and lanes represent responsibilities of a business actor for activities in a process. A pool or a lane can be an organization, a role, or a system. Lanes may subdivide pools or other lanes hierarchically.</td>
</tr>
<tr>
<td><img src="image" alt="Start symbol" /></td>
<td>This symbol represents the starting point for a process.</td>
</tr>
<tr>
<td><img src="image" alt="End symbol" /></td>
<td>This symbol represents the termination of a process.</td>
</tr>
<tr>
<td><img src="image" alt="Activity" /></td>
<td>An Activity is a unit of work or action.</td>
</tr>
<tr>
<td><img src="image" alt="Execution order symbol" /></td>
<td>This symbol defines the execution order of activities.</td>
</tr>
<tr>
<td><img src="image" alt="Indirect execution symbol" /></td>
<td>This symbol defines an indirect execution of activity (e.g. sending/exchange of information).</td>
</tr>
<tr>
<td><img src="image" alt="Decision" /></td>
<td>This symbol represents a decision, resulting in the triggering of different activities. It typically follows an activity.</td>
</tr>
<tr>
<td><img src="image" alt="Gateway" /></td>
<td>Gateway, used to ease the readability of the flow transfers</td>
</tr>
<tr>
<td><img src="image" alt="Document" /></td>
<td>A Data Object represents information flowing through the process, such as business documents, e-mails, or letters</td>
</tr>
<tr>
<td><img src="image" alt="External process" /></td>
<td>Indicates reference to an external process not described in the current business process map</td>
</tr>
</tbody>
</table>
7.2 Programme Plan Preparation, Adaptation and Assessment Review Process

Programme Plan Preparation and Assessment process (T2S.PMO.PMF.000).vsd

Decision Taking (Schedule 4, Section 13)

Steering Level Bodies
NECSG/CSG
PMG
T2S Board

Prepare Plan & Status report

Any processes (e.g. MCR) having an impact on the plan

Yes

Consensus?

Disagreement Resolution Process (T2S.PMO.PMF.040)

No

Yes

Any processes (e.g. in a PMG substructure) having an impact on the plan

Agreed

Review Plan & Status report

No

Yes

Assess need to refine T2S Programme Plan

Confirm need to refine T2S Programme Plan

Agreed

Need refinement

Yes

Assess Plan & Status report

No

Need to review T2S Programme Plan

Assess Plan & Status report

No
### 7.2.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
</table>
| T2S Programme Office | The T2S Programme Office is responsible for collecting information from the Eurosystem, Contracting CSDs and Contracting CBs in order to prepare for PMG and Steering Level review:  
  - An updated T2S Programme Plan;  
  - A Programme Status Report (including progress, risks and issues).  
The T2S Programme Office sends the relevant information (T2S Programme Plan and Programme Status Report) to the PMG, at least 1 week before PMG meetings. The T2S Programme Office is responsible for organising and chairing the PMG meetings. |
| PMG                | In this process, the PMG is responsible for:  
  - Assessing and agreeing on the updates of the T2S Operational Plan  
  - Assessing and agreeing on the T2S Programme status report.  
Its responsibility is to analyse the plan and the reporting packages, propose improvements or changes, and highlight risks and issues. When alternatives for solving an issue exist, the PMG will assess them and propose the best way forward.  
It is the responsibility of the PMG to act pro-actively and in good faith to try to achieve agreement between PMG members. |
| CSG                | The CSG is responsible for assessing the programme plan and programme status, taking into account the recommendations supplied by the PMG and taking all necessary steps to reach a consensus at Steering Level. |
| T2S Board          | The T2S Board is responsible for assessing the programme plan and programme status, taking into account the recommendations supplied by the PMG and taking all necessary steps to reach a consensus at Steering Level. The T2S Board also coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3. |
7.2.2 High-Level Process Description

This section provides an overview of the process to monitor the T2S Programme Plan. This includes progress and risk reporting, and adaptation to the plan. This process encompasses the ongoing monitoring of the programme by the different actors. It applies to production of the programme status reports and to updates of the plan. It may also result in changes to the different supporting documents, e.g. to document changes in planning assumptions. This process does not apply to changing the layouts of plans and supporting documents, as described in the Annexes of this Schedule 2. Such changes follow the process for the adaptation of Schedules described in section 7.3.

The T2S Programme Office collects information from the Eurosystem, Contracting CSDs and Contracting CBs for plan updates and status reporting.

Based on the information received, the T2S Programme Office updates the T2S Operational Plan, prepares a Programme status reports.

When applicable, the T2S Programme Office prepares presentations on changes, impacts and alternative solutions.

The T2S Programme Office sends the various plans and the programme status report to the PMG at least one week before the meeting.

The T2S Programme office presents the overall programme plan and status during the PMG sessions for review and discussion.

Once the PMG has reviewed and agreed on the T2S Operational Plan and status reports, it forwards the plan and status reports to the Steering Level for endorsement. The T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.

In case of disagreement on the implementation, the PMG may initiate the PMG disagreement resolution process in order to seek for guidance from the Steering Level.

The PMG meets at least quarterly or as agreed with the PMG members.
7.3 Adaptation Process for updated Annexes without affecting the plan:

7.3.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>T2S Programme Office</td>
<td>The T2S Programme Office is responsible for:</td>
</tr>
<tr>
<td></td>
<td>- identifying and raising adaptation requests;</td>
</tr>
<tr>
<td></td>
<td>- collecting adaptation requests;</td>
</tr>
<tr>
<td></td>
<td>- undertaking the impact assessment for the requested adaptation;</td>
</tr>
<tr>
<td></td>
<td>- communicating the results of the impact analysis to the PMG; and</td>
</tr>
<tr>
<td></td>
<td>- implementing the adaptation in the applicable processes and templates.</td>
</tr>
<tr>
<td>CSD</td>
<td>The Contracting CSDs are responsible for identifying and raising adaptation requests, if relevant.</td>
</tr>
<tr>
<td>Monitoring of Client Readiness</td>
<td>The MCR is responsible for providing information on the reasons for the adaptation request to the T2S Programme Office to allow for an impact assessment.</td>
</tr>
</tbody>
</table>
PMG | In this process, the PMG is responsible for:
- reviewing and discussing the adaptation requests;
- confirming the need of the adaptation or rejecting the request to the Steering Level; and
- escalating Disagreement on adaptation request to the Steering Level.

### 7.3.2 High Level Process Description

This section provides a process to adapt the Annexes to the present Schedule that do not affect the plan over time in a controlled way. This process is valid to change the layout of the plan and of the supporting documentation, but it does not apply for changing the plan (e.g. the Eurosystem and/or CSDs may wish to review the Annexes to Schedule 2 of this FA in order to improve reporting). Adaptations approved at Steering Level, do not need to go through this procedure, and should be directly implemented.

The T2S Programme Office and/or CSDs may wish to change an Annex.

The T2S Programme Office collects the change(s) request. Thereafter, the T2S Programme Office assesses the change(s) request. The PMG reviews the change(s) request together with the T2S Programme Office assessment.

After agreement on the change(s) at PMG level, the T2S Programme Office implements the change(s).

In case of disagreement, the PMG may initiate the disagreement resolution process to get agreement on the proposed change(s).

19 March 2014
7.4 Disagreement Resolution process

Disagreement Resolution process (T2S.PMO.PMF.040).vsd

7.4.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMG</td>
<td>The PMG is responsible for taking all necessary actions to solve the disagreement.</td>
</tr>
<tr>
<td>CSG</td>
<td>The CSG is responsible for discussing with T2S Board any disagreement escalated by the PMG and for providing guidance to the PMG. In case of outstanding disagreement after escalation at PMG level, the CSG takes all necessary steps to reach a consensus at Steering Level.</td>
</tr>
<tr>
<td>T2S Board</td>
<td>The T2S Board is responsible for discussing with CSG any disagreement escalated by the PMG and for providing guidance to the PMG. In case of outstanding disagreement after escalation at PMG level, the T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3.</td>
</tr>
</tbody>
</table>
7.4.2 High Level Process Description

This Section describes the process to be followed in case of disagreement within the PMG.

In case of disagreement within the PMG, the PMG escalates to the Steering Level for guidance on how to mitigate the disagreement.

The Steering Level discussed the escalated issue in view of providing guidance to the PMG.

The Parties should aim to conducting the process of resolving disagreements within 2 weeks.

In case of outstanding disagreement after escalation at PMG level, the T2S Board coordinates the work at Steering Level to reach a consensus following the process described in Schedule 8, Section 1.3, before a potential escalation.
FRAMEWORK AGREEMENT

SCHEDULE 2 – ANNEXES 1-10

The latest version of Schedule 2 Annexes is available [here](#).
FRAMEWORK AGREEMENT

SCHEDULE 3

USER TESTING
Table of contents

Introduction ................................................................................................................................................1
  1.1 Context ...........................................................................................................................................1
  1.2 Structure of Schedule .....................................................................................................................1

2 Scope and Objectives ............................................................................................................................2
  2.1 Scope ...............................................................................................................................................2
  2.2 Objectives .......................................................................................................................................2

3 General Responsibilities of the Contracting Parties ........................................................................4
  3.1 General responsibilities of the Eurosystem ....................................................................................4
  3.2 General responsibilities of the Contracting CSD ..........................................................................5
  3.3 General responsibilities of the PMG Substructure .........................................................................6
  3.4 General responsibility related to Monitoring Client Readiness ......................................................7

4 User Testing Preparation Phase ........................................................................................................8

5 User Testing Execution Phase .............................................................................................................9
  5.1 Testing Stage Organisation .............................................................................................................9
  5.2 Connectivity Testing Stage .............................................................................................................10
    5.2.1 Description ..............................................................................................................................10
    5.2.2 Responsibilities ......................................................................................................................10
    5.2.3 Entry Criteria ..........................................................................................................................11
    5.2.4 Exit Criteria ............................................................................................................................11
  5.3 CSDs’ Acceptance Testing Stage .....................................................................................................12
    5.3.1 Description ..............................................................................................................................12
    5.3.2 Responsibilities ......................................................................................................................12
    5.3.3 Entry Criteria ..........................................................................................................................13
    5.3.4 Exit Criteria ............................................................................................................................13
  5.4 Bilateral Interoperability Testing Stage ............................................................................................14
    5.4.1 Description ..............................................................................................................................14
    5.4.2 Responsibilities ......................................................................................................................14
    5.4.3 Entry Criteria ..........................................................................................................................14
    5.4.4 Exit Criteria ............................................................................................................................15
    5.4.5 CSD Certification ....................................................................................................................16
      5.4.5.1 Description .......................................................................................................................16
Framework Agreement

Schedule 3 – User Testing

5.4.5.2 Responsibilities ................................................................................................. 17
5.4.5.3 Entry Criteria ..................................................................................................... 18
5.4.5.4 Exit Criteria ...................................................................................................... 18

5.5 Multilateral Interoperability Testing Stage ............................................................. 19
5.5.1 Description ........................................................................................................... 19
5.5.2 Responsibilities .................................................................................................. 19
5.5.3 Entry Criteria ..................................................................................................... 19
5.5.4 Exit Criteria ....................................................................................................... 19

5.6 Community Testing Stage ....................................................................................... 20
5.6.1 Description ........................................................................................................ 20
5.6.2 Responsibilities .................................................................................................. 20
5.6.3 Entry Criteria ..................................................................................................... 21
5.6.4 Exit Criteria ....................................................................................................... 21
5.6.5 DCP Certification ............................................................................................... 22
5.6.5.1 Description ...................................................................................................... 22
5.6.5.2 Responsibilities ............................................................................................... 23
5.6.5.3 Entry Criteria .................................................................................................. 23
5.6.5.4 Exit Criteria .................................................................................................. 24

5.7 Business Day Testing Stage .................................................................................... 24
5.7.1 Description ........................................................................................................ 24
5.7.2 Responsibilities .................................................................................................. 24
5.7.3 Entry criteria ...................................................................................................... 25
5.7.4 Exit criteria ....................................................................................................... 25

6 Non-functional tests .................................................................................................. 27
6.1 Description ............................................................................................................ 27
6.2 Objectives and responsibilities of performance and stress tests ......................... 27
6.3 Objectives and responsibilities of Business Continuity tests ............................. 28
6.4 Objectives and responsibilities of Security Tests .................................................. 29
6.5 Performance Tests by CSDs .................................................................................. 29

7 User Testing Business Processes ............................................................................. 30
7.1 User Testing Stage Transition Monitoring Process ............................................. 31
7.1.1 Process Actors and their Roles .......................................................................... 32
7.1.2 Process Description .......................................................................................... 33
7.2 User Testing Stage Transition Assessment Process ............................................. 34
7.2.1 Process Actors and their Roles .......................................................................... 35
Framework Agreement

Schedule 3 – User Testing

7.2.2 Process Description ................................................................................................... 36
7.3 User Testing Stage Transition Bilateral Escalation Process ........................................ 37
  7.3.1 Process Actors and their Roles ................................................................................ 38
  7.3.2 Process Description ................................................................................................ 38
7.4 User Testing Suspension Process ................................................................................ 39
  7.4.1 Process Actors and their Roles ................................................................................ 40
  7.4.2 Process Description ................................................................................................ 40
7.5 Release Management during the User Testing ............................................................. 42
7.6 Supporting Processes .................................................................................................. 42
  7.6.1 IT Service Management processes ....................................................................... 42
8 Post-Migration Testing ........................................................................................................ 43
Annex 1 - Mapping of testing activities on the test environments ....................................... 1
1 **Introduction**

1.1 **Context**

A prerequisite for a secure and smooth transfer of settlement activities from the CSDs’ proprietary IT environments to T2S is the thorough testing of T2S in combination with the IT systems of the T2S Actors. In this context, the Contracting CSD and the Eurosystem shall cooperate in good faith for the preparation and execution of all User Testing activities according to the T2S Programme Plan and its milestones.

1.2 **Structure of Schedule**

The Schedule 3 consists of the following sections and Annexes:

- Section 1 is the introduction.
- Section 2 defines the scope and the objective of User Testing.
- Section 3 presents the general responsibilities of the Eurosystem, the Contracting CSD and the PMG substructure for User Testing.
- Section 4 describes the objectives of the User Testing preparation phase and the responsibilities of the Eurosystem and the Contracting CSD during this phase.
- Section 5 describes the structure of the testing stages for the User Testing execution phase with the respective entry and exit criteria for each testing stage as well as the conditions for transitioning between testing stages.
- Section 6 presents the description, objectives and responsibilities for the non-functional testing.
- Section 7 presents the business processes required to support the successful completion of User Testing including the stage transition process.
- Section 8 presents the post-migration testing.
- Annex 1 describes the mapping of the testing activities on the test environments.
2 Scope and Objectives

2.1 Scope

The scope of User Testing comprises functional testing and non-functional testing that the Contracting CSD and its community perform in view of assessing:

- the ability to connect to T2S (connectivity testing);
- the compliance of T2S with the T2S Services as defined in Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents (CSDs’ Acceptance Tests of the T2S Services);
- the ability to interact properly with T2S (bilateral and multilateral interoperability testing as well as community and business day testing) without negative impact on the T2S Platform or other connected parties (CSD certification and DCP certification);
- the ability to migrate CSD Static Data and Transactional Data from its legacy systems onto T2S (migration testing, mainly assessed during bilateral interoperability testing and community testing);
- the ability to extract CSD Static Data and Transactional Data from T2S for reverse migration; and
- the readiness of operational procedures for live operations.

Although the functional and non-functional tests that the Eurosystem performs do not fall into the scope of User Testing, evidence provided through these tests may be used on a discretionary basis by CSDs as a means to limit their efforts during User Testing.

2.2 Objectives

The objectives of the User Testing are:

- to provide evidence that the T2S Platform meets the user requirements, as defined by the most recently approved version of the most detailed document of the T2S Scope Defining Set of Documents and Schedule 5 (T2S Service Description);
- to ensure readiness of the Contracting CSD and its community as well as its Central Bank
and Payment Banks for the Migration to and operation on the T2S Platform;

- to allow the Contracting CSD to verify and ensure its compliance with Legal and Regulatory Requirements during the Operational Phase of T2S.
3 General Responsibilities of the Contracting Parties

This section defines the respective responsibilities of the Eurosystem, the Contracting CSD and the PMG substructure for the preparation and execution of all User Testing activities. This Schedule does not define the roles and responsibilities of the Central Banks, whose currency is available for settlement in T2S, nor of the Payment Banks, but defines the responsibility both of the Eurosystem to ensure that these T2S Stakeholders fulfil their obligations and of the Contracting CSD towards its community.

3.1 General responsibilities of the Eurosystem

The following specifies the general responsibilities of the Eurosystem with regard to the preparation and execution and completion of the User Testing activities:

i. The Eurosystem is responsible for coordinating the User Testing activities and communication between the Contracting CSD and the Central Banks whose currencies are available for settlement in T2S as well as between the Contracting CSD and other CSDs participating in the User Testing activities;

ii. The Eurosystem shall ensure that the User Testing of the Central Banks does not place restrictions on the CSDs testing;

iii. The Eurosystem shall actively take all necessary actions required to facilitate, monitor and support the adequate participation of the Central Banks whose currency is available for settlement in T2S in the testing activities of the Contracting CSD;

iv. The Eurosystem is responsible for preparing and executing the Eurosystem Acceptance Testing (EAT), and for providing regular progress reporting as well as an assessment report confirming the compliance of T2S with the T2S Scope Defining Set of Documents and Schedule 5 (T2S Service Description) before the start of User Testing;

v. The Eurosystem shall provide the reasonable support for testing activities of the Contracting CSD in the different stages of User Testing;

vi. The Eurosystem shall inform the Contracting CSD, in a timely manner, about any developments that may prevent that CSD or its DCP(s) from completing its/their testing activities, and shall propose identified mitigation measures;
vii. The Eurosystem shall ensure that a PMG substructure is in place, in accordance with the T2S governance framework (section 2.4 of Schedule 8 - Governance), for the planning, coordination and monitoring of the User Testing activities;

viii. The Eurosystem shall reconcile and consolidate the individual status reports of CSDs and Central Banks on the progress of their User Testing activities and shall provide a regular status update based on this consolidation to the Contracting CSD through the PMG substructure;

ix. The Eurosystem shall investigate and reconcile different test outcomes by different CSDs or DCPs for delivering a consolidated list of defects to the PMG substructure;

x. The Eurosystem shall undertake the configuration of test environments for the different testing stages as agreed with the PMG substructure. The Eurosystem will provide the necessary data configurations to ensure the logical segregation of data for the test activities of CSDs;

xi. The Eurosystem is responsible for maintaining configuration parameters and the User Testing Calendar (settlement day calendar, operating hours, cut-off times, etc.) for each test environment as agreed with the PMG substructure for User Testing;

xii. Based on the principles of ITIL V3 Service Operation, the Eurosystem shall establish and operate the necessary IT service management processes that include a defect resolution process to remedy errors;

xiii. The Eurosystem shall operate T2S in accordance with the SLAs for User Testing as defined in Schedule 6 (T2S Service Level Agreement).

3.2 General responsibilities of the Contracting CSD

The following specifies the general responsibilities of the Contracting CSD for the preparation and execution of the User Testing activities:

i. The Contracting CSD is responsible for the communication with its community regarding User Testing;

ii. The Contracting CSD is responsible for ensuring the timely completion of all its testing activities and shall report its findings on the execution of its test cases and test scenarios to the Eurosystem on a regular basis;
iii. The Contracting CSD is responsible for supporting and monitoring the timely completion of the testing activities of its community, and specifically of its Directly Connected Parties (DCPs);

iv. The Contracting CSD appoints a single point of contact for all topics related to the User Testing representing the Contracting CSD in the PMG substructure;

v. The Contracting CSD, independent of its migration wave and even after having completed its own testing, shall support other CSDs and CBs in testing of T2S;

vi. The Contracting CSD shall inform the Eurosystem, in a timely manner, about any developments, which may prevent that CSD or its DCP(s) from completing its/their testing activities;

vii. The Contracting CSD shall provide reasonable support to the Eurosystem by providing information on test outcomes;

viii. The Contracting CSD shall participate in the PMG substructure in charge of User Testing as required to ensure the proper functioning of this body and the smooth coordination of the User Testing activities.

3.3 General responsibilities of the PMG Substructure

The PMG substructure shall be composed of the Participating CSDs, euro area NCBs, participating non-euro area NCBs, the 4CB and the ECB. The following specifies the general responsibilities of the PMG substructure in the preparation and execution of the User Testing activities for the initial T2S go-live and new software releases after T2S go-live of the final migration wave that the substructure shall be responsible for:

i. Meet (physically or via conference call) on a regular basis and on an ad hoc basis when requested by one of the members to prepare, plan, coordinate, monitor and review User Testing activities. The PMG substructure determines the frequency of its meetings based on its needs;

ii. Prepare, update and agree the User Testing Calendar in accordance with the T2S Programme Plan;

iii. Decide on changes to the opening / closing times of the testing environments and operational hours in line with the provisions of the SLA;

iv. Review the consolidated User Testing status reports from the Eurosystem on the overall
progress of CSDs, Central Banks and their respective communities on User Testing;

v. Review the list of incidents;

vi. Review the software defects, classify the software defects and agree on the contents of a package for a T2S release on the User Testing environments;

vii. In the case that the PMG substructure cannot reach an agreement, it may escalate to the PMG;

viii. Prepare communication on the progress of User Testing via the PMG to the Steering Level;

ix. Coordinate and monitor the participation of the various T2S Actors (Eurosystem, CSDs and non-euro area NCBs, DCPs and Payment Banks) during the different stages of testing. At its own discretion, the CSD may coordinate testing activities directly with other T2S Actors when it does not conflict with the agreed approach of the PMG substructure;

x. Identify, manage, report and escalate risks and issues related to User Testing according to the ‘Programme Plan Preparation, Adaptation and Assessment Review Process’ in section 7.2 of Schedule 2 (T2S Programme Planning and Monitoring);

xi. Request plan changes related to User Testing according to the ‘Programme Plan Preparation, Adaptation and Assessment Review Process’ in section 7.2 of Schedule 2 (T2S Programme Planning and Monitoring);

xii. Request adaptations of User Testing items documented in Annexes 4 to 10 of Schedule 2, according to the ‘Adaptation Process for updated Annexes without affecting the plan’ in section 7.3 of Schedule 2 (T2S Programme Planning and Monitoring);

xiii. Take or request decisions on User Testing related topics according to the decision-making process defined in section 1.3 of Schedule 8 (Governance).

3.4 General responsibility related to Monitoring Client Readiness

The monitoring and reporting of the progress of an individual CSD with its client relationship manager during User Testing will follow the framework for Monitoring Client Readiness (MCR) as defined in Schedule 2 (T2S Programme Planning and Monitoring).
4 User Testing Preparation Phase

The objective of the User Testing preparation phase is to:

- organise processes and activities required for the User Testing execution phase, as defined in section 7 of this Schedule;
- undertake an initial risk assessment for the User Testing execution phase as specified by the Schedule 2 risk management framework to ensure the subsequent proactive risk management by the PMG substructure;
- prepare and design all necessary test documentation and testing processes, e.g. User Testing Calendar, test cases for certification, test data.

In this preparation phase for User Testing, the Eurosystem with the support of the Contracting CSD through its participation in the PMG substructure for User Testing establishes the required process framework and prepares the agreed deliverables for the User Testing execution phase.

The responsibilities of the Eurosystem in this phase are:

i. to establish the processes required for the User Testing execution phase, as defined in Section 7 of this Schedule;
ii. to develop a training programme for T2S and deliver a reasonable amount of training to the Contracting CSD;
iii. to prepare and provide the prerequisite deliverables for the Contracting CSD to prepare its User Testing, e.g. the User Testing Process Guide, the Registration Guide, the Connectivity Guide, and the Manual of Operational Procedures;
iv. to provide to the Contracting CSD the sets of Eurosystem Acceptance Testing (EAT) functional test cases and test scenarios for information purposes, as an input for the Contracting CSD’s test preparation.
In this preparation phase for User Testing, the responsibilities of the **Contracting CSD** are:

i. to support the Eurosystem in the preparation of the overall User Testing Calendar by providing the Eurosystem with its proposed test plan and testing calendar of its activities;

ii. to comply with the processes for User Testing, as defined in Section 7 of this Schedule.

### 5 User Testing Execution Phase

This section describes the structure of the testing stages for User Testing execution phase with the respective entry and exit criteria for each testing stage as well as the conditions for transitioning between testing stages.

#### 5.1 Testing Stage Organisation

The User Testing execution phase consists of both independent and sequenced testing stages. The purpose of the different testing stages is to increase gradually the number of T2S Actors involved and expand the scope of the testing.
5.2 Connectivity Testing Stage

5.2.1 Description

Establishing the technical connectivity to a test environment is the first stage of User Testing. This is required for each environment that the Contracting CSD uses for testing, however, the connectivity testing stage is the initial verification that the systems of both the Contracting CSD and the Eurosystem can communicate successfully on the technical and application level. The Contracting CSD shall repeat these tests for each connectivity channel it intends to use while the connection to further T2S test environments might have a reduced connectivity test scope.

The scope of connectivity testing consists of:

- testing the ability to reach the welcome pages of the U2A interface and performing the login to the system;
- exchange of messages on application level;
- push-and-pull services for reports.

5.2.2 Responsibilities

The following set of responsibilities shall apply for the connectivity testing stage:

i. The Eurosystem shall support the connectivity testing of the Contracting CSD and the DCPs;

ii. The Contracting CSD shall acquire T2S specific network Connectivity Services and ensure the timely readiness of its connection to the relevant T2S test environment(s);

iii. The Contracting CSD together with the Eurosystem will evaluate the test results at the end of the connectivity testing stage to assess the fulfilment of the exit criteria for this testing stage.
5.2.3 Entry Criteria

The following conditions shall apply for the start of the connectivity testing stage:

- The Eurosystem has confirmed the successful achievement of synchronisation point 4 (Network Providers Confirmed for VAN);

- The Eurosystem has confirmed the successful achievement of synchronisation point 7 (Ready to Start Connectivity Set-up);

- The Contracting CSD has completed the preparation to setup the network connection for the User Testing environments, according to the NSP user documentation;

- The Contracting CSD has adapted its IT system according to the T2S Scope Defining Set of Documents.

5.2.4 Exit Criteria

The following conditions shall apply for the successful conclusion of the connectivity testing stage:

- The Contracting CSD confirms to the Eurosystem that its IT platform can successfully exchange message-based communication and receive pushed messages on application level with T2S;

- The Contracting CSD confirms the correct setup of communication parameters and security features with its Network Service Provider(s) in order to communicate with the T2S test environment(s).
5.3 CSDs’ Acceptance Testing Stage

5.3.1 Description

The CSDs’ acceptance testing stage is the period of up to 6 months within the User Testing execution phase reserved for CSDs to confirm that T2S complies with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents. Independently from its migration wave, the Contracting CSD may start its acceptance testing when the Eurosystem confirms its successful achievement of synchronisation point 8 (Start Bilateral Interoperability Testing (for all waves)).

The CSDs’ Acceptance Tests of the T2S Services\(^1\) are bilateral between the Eurosystem and the Contracting CSD. The T2S Compliance Confirmation of one CSD does not prejudge the agreement by other CSDs. Executing this testing stage is optional. The Contracting CSD may rely on its test results from its bilateral and multilateral interoperability testing as well as those from its CSD certification testing. Regardless of how a CSD undertakes this testing stage, in case the Contracting CSD choses to execute acceptance testing, the Contracting CSD is required to confirm that T2S is compliant with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents. Article 17 of the Framework Agreement defines the possible consequences of T2S non-conformity based on the results of the CSDs’ Acceptance Tests of the T2S Services.

In order for the Contracting CSD to obtain certainty that T2S fulfils the non-functional user requirements, the Eurosystem will prepare and execute non-functional tests based on test cases that will be shared with the Contracting CSD for a quick consultation before the start of non-functional testing by the Eurosystem. The Eurosystem will deliver a test report with the results of the test execution according to the defined scope of the non-functional tests.

5.3.2 Responsibilities

The following set of responsibilities shall apply for the CSDs’ acceptance testing stage:

i. In the context of the framework set out in Schedule 2 (T2S Programme Planning and Monitoring) on the monitoring of client readiness, the Eurosystem and the Contracting

\(^1\) The term “CSDs’ Acceptance Tests of the T2S Services” does not indicate that the T2S Services imply any element of a contract for work under German law. Chapter 2 of this Agreement defines the rights and obligations of the Parties that describe the T2S Services.
CSD shall have regular contact to review the progress of the CSDs’ acceptance testing stage;

ii. The Contracting CSD has the obligation to provide regular reporting on the results of its tests in the form of status reports to the Eurosystem. This report shall cover at minimum the number of test cases and test scenarios successfully executed and failed (cases of non-compliance) with the Contracting CSD’s assessment of the criticality of identified defects and corresponding measures to compensate for potential delays, when required;

iii. The Contracting CSD has the obligation to provide evidence, if it intends not to accept T2S because of failed test cases, that the respective test cases comply with the T2S Scope Defining Set of Documents and Schedule 5 (T2S Service Description);

iv. Based on the bilateral status reporting from the Contracting CSD, the Eurosystem shall monitor the testing. The Eurosystem shall share information about the progress and results of the CSDs’ Acceptance Tests of the T2S Services with the CSDs via the PMG substructure on a consolidated basis;

v. The Contracting CSD together with the Eurosystem will evaluate the test results at the end of the CSDs’ acceptance testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.3.3 Entry Criteria

The following condition shall apply for the start of the CSDs’ acceptance testing stage:

- The Eurosystem has confirmed the successful achievement of synchronisation point 8 (Start Bilateral Interoperability Testing (for all waves)).

5.3.4 Exit Criteria

The following condition shall apply for the end of the CSDs’ acceptance testing stage:

- The criterion for a CSD to exit the CSDs’ acceptance testing stage shall be its declaration that T2S complies with Schedule 5 (T2S Service Description) and the T2S Scope Defining Set of Documents.
5.4 Bilateral Interoperability Testing Stage

5.4.1 Description

In the bilateral interoperability testing stage, the Contracting CSD tests T2S to ensure the readiness of its adapted IT system to interoperate with T2S and verifies that all T2S Services in T2S are working as required. It undertakes its testing without interacting with other Participating CSDs and Central Banks. T2S ensures the segregation of the testing activities of the Contracting CSD from other CSDs’ test activities on T2S by creating a set of fictitious CSDs and Central Banks under which the Contracting CSD can operate. The objective of this testing stage is to ensure that the CSDs’ adapted IT system can interoperate with T2S properly before testing with other CSDs and Central Banks. A CSD can continue performing bilateral testing even when it undertakes multilateral testing.

5.4.2 Responsibilities

The following set of responsibilities shall apply for the bilateral interoperability testing stage:

i. The Eurosystem shall establish the operational procedures and service management required to support the bilateral interoperability testing stage;

ii. The Contracting CSD is responsible for organising its bilateral interoperability testing stage in line with the User Testing Calendar;

iii. The PMG substructure shall be responsible for monitoring the bilateral interoperability testing stage;

iv. The Contracting CSD shall test the migration processes (loading CSD Static Data, loading Transactional Data, migration weekend rehearsals, reverse migration, etc.);

v. The Contracting CSD together with the Eurosystem will evaluate the test results at the end of the bilateral interoperability testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.4.3 Entry Criteria

The following conditions shall apply for the start of the bilateral interoperability testing stage:

- The Contracting CSD has completed the connectivity testing stage successfully;
The Eurosystem has provided the EAT Assessment Report four weeks before synchronisation point 8 (Start Bilateral Interoperability Testing (for all waves)), covering the full scope of Eurosystem Acceptance Testing and confirming that the Eurosystem considers T2S being ready for start of User Testing;

- The Eurosystem has resolved all reported defects classified with critical severity, identified during EAT. Except otherwise agreed between the Parties, the Eurosystem has resolved all recorded defects classified with high severity;

- For the pending errors from the EAT, the Eurosystem has provided a timetable for implementation of software corrections and for regression testing of those corrections for those test cases that failed because of defects in T2S that are not critical;

- The Eurosystem has confirmed the successful achievement of synchronisation point 8 (Start Bilateral Interoperability Testing (for all waves));

- The Eurosystem has delivered to the Contracting CSD preliminary evidence that the future T2S production environment will meet the non-functional requirements based on the results of the T2S non-functional tests. The Eurosystem executes these tests in the future T2S production environment;

- The Eurosystem has confirmed its operational readiness to support the Contracting CSD;

- The Contracting CSD has confirmed its readiness to start User Testing;

- The Eurosystem and the Contracting CSD have confirmed completion of the training required to ensure the smooth start of testing activities;

- The Eurosystem has provided the documentation required for migration testing and migration dress rehearsals.

### 5.4.4 Exit Criteria

The following condition shall apply for the end of the bilateral interoperability testing stage:

- The Eurosystem has certified the Contracting CSD according to the requirements in Section 5.4.5 of this Schedule.
5.4.5 CSD Certification

5.4.5.1 Description

The CSD certification, conducted during the User Testing execution phase, aims at providing evidence by the Contracting CSD that its adapted IT platform does not harm T2S as the result of inappropriate technical communication or procedures. It runs in parallel to the bilateral interoperability testing stage. The Contracting CSD’s participation in the CSD certification testing is mandatory. Certification shall require the Contracting CSD to execute a mandatory set of tests, agreed through the PMG substructure during the User Testing preparation phase. The Eurosystem may exempt the Contracting CSD from performing mandatory test cases that are not in the scope of the Contracting CSD’s intended usage of T2S. The Contracting CSD may rely on its test results from its bilateral testing to document its completion of a mandatory certification test case.

CSD certification is bilateral between the Eurosystem and the Contracting CSD. The Eurosystem shall provide written confirmation to the Contracting CSD after determining whether the Contracting CSD has successfully completed its assigned set of mandatory certification test cases, based on a formal report from the Contracting CSD in which the Contracting CSD shall document its fulfilment of the predefined CSD certification testing exit criteria. The Eurosystem shall retain as evidence for proper certification the Contracting CSD’s formal report as well as the Contracting CSD’s progress reports on its certification testing and reporting on the level of the test cases and test scenarios.

The certification of the Contracting CSD shall remain valid until:

- the Eurosystem deploys a major release with a significant scope change in the A2A interface or major structural changes to the processing model and/or data model; or
- the Contracting CSD has made major changes to its interface processing for T2S.

In the first case, the Eurosystem shall recommend to the Steering Level whether the new release requires a re-certification of the Participating CSDs and CBs, based on the scope of the changes that the Change Review Group (CRG) has approved for the new T2S release. In the latter case, the Contracting CSD shall assess the scope of the changes and shall decide whether it must undertake re-certification testing.
5.4.5.2 Responsibilities

The following set of responsibilities shall apply for the CSD certification testing:

i. The Eurosystem shall deliver for review to the Contracting CSD through the PMG substructure the test scenarios and test cases that the Contracting CSD has to execute successfully to achieve its certification;

ii. The Eurosystem shall consult the PMG substructure on the test cases and test scenarios for CSD certification to ensure and agree the proper scope coverage;

iii. In the context of the framework set out in Schedule 2 on the monitoring of client readiness, the Eurosystem and the Contracting CSD shall have regular contact to review the progress of the CSD’s certification testing;

iv. The Contracting CSD shall execute the mandatory test cases and test scenarios for certification within the period foreseen in the T2S Programme Plan for the migration wave in which it is participating;

v. The Contracting CSD has the obligation to provide regular reporting on the results of its certification tests in the form of status reports to the Eurosystem, documenting its progress with, at minimum, the number of test cases and test scenarios successfully executed and failed;

vi. Based on the bilateral status reporting from the Contracting CSD, the Eurosystem shall monitor the certification testing. The Eurosystem shall share information about the progress of and results of the CSDs’ certification with the CSDs via the PMG substructure on a consolidated basis;

vii. Based on a formal report from the Contracting CSD, the Eurosystem will evaluate the results of the CSD’s certification testing to assess whether the Contracting CSD executed the certification test cases completely and successfully;

viii. The Eurosystem will issue the CSD Certificate for the Contracting CSD when the Eurosystem assesses that the Contracting CSD has executed the certification test cases completely and successfully.
5.4.5.3 Entry Criteria

The following conditions shall apply for the start of the CSD certification:

- The Contracting CSD has completed the connectivity testing stage successfully;

- As specified in the T2S Programme Plan, the Eurosystem has delivered to the Contracting CSD its test scenarios and test cases that the Contracting CSD is to execute for its certification;

- The PMG substructure has assessed the test cases and test scenarios for CSD certification to ensure proper scope coverage.

5.4.5.4 Exit Criteria

The following conditions shall apply for the successful conclusion of the CSD certification:

- The Contracting CSD has provided evidence of its successful completion of the mandatory certification test cases and test scenarios;

- The Eurosystem has confirmed in writing to the Contracting CSD that the Contracting CSD has successfully completed all tests required for certification.
5.5  Multilateral Interoperability Testing Stage

5.5.1 Description

In the multilateral interoperability testing stage, the Contracting CSD tests with other Participating CSDs and Central Banks of its migration wave and of previous migration waves. The multilateral interoperability testing stage is the stage in which Participating CSDs of a migration wave begin to test their settlement links with each other and Participating CSDs of a previous migration wave. In this stage, the Contracting CSD also begins the set-up and testing of configuration data and parameters for the intended production set-up (e.g. message subscriptions, cross-CSD links).

5.5.2 Responsibilities

The following set of responsibilities shall apply for the multilateral interoperability testing stage:

i. The PMG substructure shall be responsible for the planning and coordination of the multilateral interoperability testing stage;

ii. The Contracting CSD shall support the Participating CSDs of its own migration wave and of subsequent migration waves when it has links to those Participating CSDs;

iii. The PMG substructure will evaluate the test results at the end of the multilateral interoperability testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.5.3 Entry Criteria

The following conditions shall apply for the start of the multilateral interoperability testing stage:

- The Contracting CSD has completed its CSD certification successfully and confirmed its readiness to start multilateral interoperability testing;

- The PMG substructure has assessed the User Testing Stage Report detailing the severity of all defects reported during the bilateral interoperability testing stage and not yet resolved.

5.5.4 Exit Criteria

The following conditions shall apply for the end of the multilateral interoperability testing stage:

- The PMG substructure determines that the Participating CSDs of a migration wave have successfully completed multilateral interoperability testing;
No critical software bugs or operational issues remain open. The Eurosystem has resolved all reported defects classified with critical severity. Except the Parties agree otherwise, the Eurosystem has resolved all recorded defects, classified with high severity;

The PMG substructure has agreed a timetable for implementation of software corrections and for regression testing of those corrections for those test cases that failed because of non-critical defects in T2S.

5.6 Community Testing Stage

5.6.1 Description

The community testing stage is the stage in which the Contracting CSD of a migration wave extends its multilateral testing activities with other Participating CSDs and Central Banks to its community, i.e. the group of T2S Users having a contractual relationship with the Contracting CSD. The main objective of this stage is to validate that the Contracting CSD’s participants can interact correctly end-to-end with T2S, either through the Contracting CSD’s adapted systems or with T2S directly as DCP.

During the testing stage CSDs and their communities verify the correct functioning of T2S using the target data configuration as configured for the target production environment. The expectation is that processing errors will stem mainly from incorrect data configurations, allowing the Contracting CSD to identify and correct such incorrect configurations, and from DCPs’ testing of their interface to T2S. This stage represents the first opportunity of the Contracting CSD’s participants to test with T2S, allowing the CSD’s participants to verify that their system interoperate correctly with T2S.

The community testing stage allows the Contracting CSD and its community to familiarise themselves with operational procedures and service management relevant to this stage to ensure that the operational procedures as described in the Manual of Operational Procedures (MOP) are working as expected.

5.6.2 Responsibilities

The following set of responsibilities shall apply for the community testing stage:

i. The Contracting CSD shall test the migration process (loading CSD Static Data, loading Transactional Data, migration weekend rehearsals, reverse migration, etc.) together with its community;

ii. The Contracting CSD shall involve its T2S Users and other relevant T2S Stakeholders in the testing activities in order to validate the end-to-end business processes supported
iii. The Contracting CSD together with the Eurosystem will evaluate the test results at the end of the community testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.6.3 Entry Criteria

The following conditions shall apply for the start of the community testing stage:

- The Contracting CSD has exited the CSDs’ acceptance testing and the multilateral interoperability testing stage successfully and declared its operational readiness for community testing;
- The Eurosystem has confirmed the readiness of its operational teams;
- The Eurosystem has confirmed the readiness of the required Central Banks and their holders of Dedicated Cash Accounts in the tests;
- The PMG substructure confirms the successful completion of multilateral interoperability testing stage of the applicable migration wave and that the community testing stage can start.

5.6.4 Exit Criteria

The following conditions shall apply for the successful conclusion of the community testing stage:

- The PMG substructure determines that the CSDs of a migration wave, together with their communities and the relevant Central Banks of the CSDs have successfully executed the migration rehearsals and business days;
- No critical software bugs or operational issues remain open that constitute a significant risk to the go-live of the migration wave. The Eurosystem has resolved all reported defects classified with critical severity. The Eurosystem has resolved all recorded defects classified with high severity except when otherwise agreed between the Parties;
- The PMG substructure has agreed a timetable for implementation of software corrections and for regression testing of those corrections for those test cases that failed because of defects in T2S that are not critical;
The DCP(s) of the Contracting CSD has/have successfully completed all tests related to its/their DCP certification;

The relevant operational and the incident management procedures of the Contracting CSD and its community have been carried out successfully;

The CSDs and Central Banks (of the CSDs) of the respective migration wave confirm their readiness to progress to the business day testing stage.

5.6.5 DCP Certification

5.6.5.1 Description

The DCP certification aims at providing evidence by the participant of the Contracting CSD that its adapted IT platform does not harm T2S as the result of inappropriate technical communication or procedures. DCP certification does not verify the compliance with either the Contracting CSD’s adaptation to T2S nor with the Contracting CSD’s business processing requirements. When conducted during the User Testing execution phase, it runs in parallel to the community testing stage for those participants of the Contracting CSD that request to connect directly to T2S. Participants of the Contracting CSD also have the option to undertake their DCP certification at any time after the Contracting CSD is operating on T2S. The DCP certification of a CSD participant shall be valid for all Contracting CSDs from which it has authorisation to connect directly to T2S. DCP certification requires connectivity testing before the DCP starts its certification testing.

DCP certification is mandatory for any participant of the Contracting CSD that chooses to connect its IT systems directly to T2S. DCP certification shall require the participant of the Contracting CSD to execute a mandatory set of tests, agreed through the PMG substructure during the User Testing preparation phase. When the Contracting CSD allows its participants to connect directly to T2S and the Contracting CSD’s participant chooses to connect directly to T2S, the Contracting CSD shall allow the Eurosystem to undertake the certification process directly with the Contracting CSD’s participant.

A CSD participant has to certify itself once with the Eurosystem to connect directly to T2S. When the Contracting CSD allows its participants to connect directly to T2S, the Contracting CSD has the obligation to accept the DCP certification of its participant even when the Contracting CSD’s participant has certified itself with the Eurosystem through another Participating CSD.
The Eurosystem may require the participant of the Contracting CSD to repeat its certification testing should the Eurosystem deploy a major release with a significant scope change in the Application-to-Application interface or major structural changes to the processing model and/or data model. The Eurosystem shall recommend to the Steering Level whether the new release requires repeating of certification testing by the DCPs based on the scope of changes that the Change Review Group (CRG) has approved for the new T2S release.

5.6.5.2 Responsibilities

The following set of responsibilities shall apply for the DCP certification testing:

i. The Eurosystem shall deliver for review to the Contracting CSD through the PMG substructure the test scenarios and test cases that a Contracting CSD’s participant has to execute successfully to achieve its DCP certification;

ii. The Eurosystem shall consult the PMG substructure on the test cases and test scenarios for DCP certification to ensure and agree the proper scope coverage;

iii. The Eurosystem shall monitor the DCP certification testing. The Eurosystem shall share information about the progress and results of the DCP certification with the CSDs via the PMG substructure on a consolidated basis;

iv. The Eurosystem shall provide written confirmation to the Contracting CSD and to its participant after determining whether the participant has successfully completed its assigned set of mandatory certification test cases;

v. The Eurosystem shall retain as evidence for proper DCP certification the documentation of the DCP’s certification testing and reporting on the level of the test cases and test scenarios.

5.6.5.3 Entry Criteria

The following conditions shall apply for the start of the DCP certification:

- The Contracting CSD has fulfilled the exit criteria for the CSDs’ acceptance testing stage;
- The Contracting CSD and the Eurosystem have fulfilled the exit criteria for the CSD certification testing;
- The Contracting CSD has authorised its respective participant to connect directly to T2S.
5.6.5.4 Exit Criteria

DCP certification has no exit criteria. However, DCP certification is the prerequisite for the Contracting CSD’s participant to take part in community testing of the Contracting CSD as a DCP.

5.7 Business Day Testing Stage

5.7.1 Description

The business day testing stage comprises the simulation of several consecutive business days of T2S operation after completing a migration rehearsal for the respective CSD migration wave using the expected production data set-up. It includes all CSDs of a migration wave and their respective communities as well as their Central Banks and their Payment Banks. CSDs and their communities from previous migration waves participate when deemed necessary, e.g. when links exist.

The objective of the business day testing stage is to verify the correct functioning of T2S under production-like conditions using the target data configuration as expected in the production environment. In this stage of testing, the expectation is that processing errors will stem mainly from incorrectly migrated data (e.g. incorrect positions or missing ISINs) or incorrect configuration (e.g. cross-CSD settlement parameters). This stage enables the T2S Actors, such as the CSDs and their communities, to identify such errors using real business data.

The business day testing stage includes operational procedures and service management to ensure that the operational procedures as described in the Manual of Operational Procedures (MOP) are working as expected.

5.7.2 Responsibilities

The following set of responsibilities shall apply for the business day testing stage:

i. The Eurosystem shall establish the operational procedures and service management required to support the business day testing stage;

ii. The Contracting CSD shall test the migration process (loading CSD Static Data, loading Transactional Data, migration weekend rehearsals, reverse migration, etc.) together with its community;

iii. The Contracting CSD shall involve its T2S Users and other relevant T2S Stakeholders in the testing activities in order to validate the end-to-end business day processes supported by T2S;
iv. The Contracting CSD together with the Eurosystem will evaluate the test results at the end of the business day testing stage to assess the fulfilment of the exit criteria for this testing stage.

5.7.3 Entry criteria

The following conditions shall apply for the start of the business day testing stage:

- The Contracting CSD has fulfilled the exit criteria for the community testing stage;
- The PMG substructure confirms that the CSDs and their Central Banks participating in the respective migration wave have fulfilled the exit criteria for community testing.

5.7.4 Exit criteria

The following conditions shall apply for the successful conclusion of the business day testing stage:

- The PMG substructure determines that the CSDs of a migration wave, together with their communities and the relevant Central Banks have successfully executed the migration rehearsals and business days;
- No critical software bugs or operational issues remain open that constitute a significant risk to the go-live of the migration wave. The Eurosystem has resolved all reported defects classified with critical severity. Except otherwise agreed between the Parties, the Eurosystem has resolved all recorded defects classified with high severity;
- The PMG substructure has agreed a timetable for implementation of software corrections and for regression testing of those corrections for those test cases that failed because of non-critical defects in T2S;
- No client systems have become inoperable due to unexpected communication received from the T2S Platform for at least 15 working days prior to the agreed Business Day testing stage exit date;
- The Eurosystem confirms that testing of operational procedures has been successful;
The PMG substructure confirms that appropriate fallback arrangements and rollback procedures are established and successfully tested for the Migration;

The CSDs and Central Banks (of the CSDs) of respective migration wave confirm their readiness to go-live on T2S.
6 Non-functional tests

This section describes the non-functional tests carried out by the Eurosystem in order to confirm non-functional compliance of T2S as well as the non-functional volume tests carried out by the CSDs.

6.1 Description

The non-functional tests aim to check the proper functioning of T2S and are composed of the following tests as defined in the General Technical Design document:

- performance and stress tests;
- business continuity tests;
- security tests.

In principal, the Eurosystem will perform the non-functional tests, involvement of CSDs varies depending on the different types of non-functional test. Prior to the execution, the Eurosystem will provide for a quick consultation these tests to the CSD. After the test execution, the Eurosystem will deliver a test report with results of those tests. Moreover, the CSDs will have the opportunity to execute non-functional tests from an end-to-end perspective and respecting the sizing of the related test environments (see also section 6.5 Performance Tests by CSDs).

6.2 Objectives and responsibilities of performance and stress tests

The main objective of the performance and stress tests is to check that the T2S production environment is able to handle the estimated volume of transactions in the peak hour in terms of the number of settlements and a certain number of concurrent interactive users in compliance with a defined response time.

The test plan for the performance and stress tests includes a global system test aimed to measure throughput, response time and resource consumption of the whole system (infrastructure and applications) and volume tests conducted on specific parts of the system in order to optimise the behaviour of these T2S components.

During the performance and stress tests, different test cases shall be performed aiming to simulate the expected daily workload profiles for User-to-Application mode (U2A) and Application-to-Application (A2A) interactions on the available interfaces by using simulators and/or with the collaboration of the Contracting CSD.
The test plan for the performance and stress tests shall follow a gradual approach to verify, in sequence, that all infrastructure components and services are sized properly to handle the defined peak workload of settlements and the T2S application is able to satisfy the defined performance requirements.

The performance and stress tests shall be performed by the Eurosystem. The T2S Actors shall be invited as observers to the performance and stress tests and the results of these tests shall be delivered to the Contracting CSD.

6.3 Objectives and responsibilities of Business Continuity tests

The main objective of the business continuity tests is to verify the ability of T2S to guarantee the continuity of business services in case of local component failure or regional disaster event. The business continuity tests shall demonstrate that T2S is sufficiently resilient to meet the agreed service levels, even in case of severe incidents. The tests include intra-region and inter-region failover tests to guarantee that the production environment(s) can be switched to another site or region in a failover situation.

The business continuity tests shall be performed before the go-live and on a regular basis after the go-live.

The test plan for the business continuity tests shall include a comprehensive list of test cases including:

- fault tolerance (i.e. resiliency of single component);
- intra-region recovery;
- inter-region recovery (only regions 1 and 2).

In addition, tests shall be performed to validate the rotation between region 1 and region 2 that is closely linked to the disaster recovery test in terms of organisation and operational procedures.

The business continuity tests shall be performed by the Eurosystem. The T2S actors shall be invited as observers to the business continuity tests and the results of these tests shall be delivered to the Contracting CSD.
6.4 Objectives and responsibilities of Security Tests

The main objectives of the security tests are to verify the compliance of the T2S Platform with the T2S security requirements. Security tests include:

- Vulnerability assessment;
- Configuration analysis;
- Penetration tests.

The Eurosystem shall perform these security tests and provide the results to the Contracting CSD.

6.5 Performance Tests by CSDs

Performance tests are typical non-functional tests that a CSD or DCP may want to perform. Depending on the intended volumes, such tests shall require central coordination and prior approval.

In case the Contracting CSD or its DCP(s) intends to exceed the pre-defined hourly volume limits, the Contracting CSD shall send a request for additional processing capacity for specific performance tests to the Eurosystem at least 5 working days in advance. The request should contain the volumes to be tested and the duration of the test. The Eurosystem will verify whether it can fulfil the request and shall inform the Contracting CSD or its DCP accordingly. If the Eurosystem cannot fulfil the request as specified, the Eurosystem shall propose alternative options in terms of dates, times and/or volumes. In case of conflicting requests, the Eurosystem shall consult the PMG substructure.
7 User Testing Business Processes

This section presents the core business processes that the Eurosystem, the Contracting CSD and the Participating CSDs shall comply with for User Testing. The business process description uses a simplified version of the Business Process Modelling Notation (BPMN) 2.0, as specified in Section 7.1 of Schedule 2 (T2S Programme Planning and Monitoring). The User Testing processes may be subject to further improvement and detailing by the PMG sub-structure for the preparation and execution of all User Testing activities during the term of this Agreement.
7.1 User Testing Stage Transition Monitoring Process

User Testing Stage Transition Monitoring Process (T2S.UT.S3.000)

<table>
<thead>
<tr>
<th>Eurosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver Documentation</td>
</tr>
<tr>
<td>Stage Transition Assessment Process (T2S.UT.S3.020)</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Implement Corrective Actions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess Status and Progress</td>
</tr>
<tr>
<td>Stage Transition Milestone?</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Identify and Assess Corrective Actions</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Disagreement?</td>
</tr>
<tr>
<td>Relevant escalation process (Bilateral/Multilateral)</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
<tr>
<td>Implement Corrective Actions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CSD/NCB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliver Documentation</td>
</tr>
<tr>
<td>Implement Corrective Actions</td>
</tr>
</tbody>
</table>
7.1.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSD / CB</td>
<td>In this process, the CSD / CB is responsible for:</td>
</tr>
<tr>
<td></td>
<td>- Providing a sufficient level of documentation to the Eurosystem to allow the Eurosystem to assess the Contracting CSD’s progress for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>- Assessing its fulfilment of the entry and exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>- Identifying and assessing the feasibility of proposed correction actions, when required; and</td>
</tr>
<tr>
<td></td>
<td>- Discussing the feasibility of the proposed corrective actions with the Eurosystem.</td>
</tr>
<tr>
<td>Eurosystem</td>
<td>In this process, the Eurosystem is responsible for:</td>
</tr>
<tr>
<td></td>
<td>- Providing a sufficient level of documentation to the CSD to allow the CSD to assess the Eurosystem’s fulfilment of the entry / exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>- Assessing its fulfilment of the entry and exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>- Identifying and assessing the feasibility of proposed correction actions, when required; and</td>
</tr>
<tr>
<td></td>
<td>- Discussing the feasibility of the proposed corrective actions with the CSDs.</td>
</tr>
<tr>
<td>Monitoring of Client Readiness (MCR)</td>
<td>In this process, the MCR:</td>
</tr>
<tr>
<td></td>
<td>- Monitors the Contracting CSD’s progress in order to determine whether it has fulfilled the entry or exit criteria for a testing stage; and</td>
</tr>
<tr>
<td></td>
<td>- Discusses and decides on the feasibility of proposed corrective actions; and</td>
</tr>
<tr>
<td></td>
<td>- Provides guidance to the PMG substructure when required in the case of multilateral escalation.</td>
</tr>
</tbody>
</table>
7.1.2 Process Description

The objective of the User Testing stage transition monitoring process is to ensure bilateral communication between the Eurosystem and the Contracting CSD on the progress of the Contracting CSD’s User Testing:

- to ensure adequate coordination of the User Testing activities;
- to enable proactive monitoring of the CSD’s fulfilment of the exit and/or entry criteria for User Testing stages; and
- to allow for an early identification of issues and corrective measures for their resolution.

Both the Contracting CSD and the Eurosystem provide progress updates for assessing the progress for the current stage of User Testing. The Eurosystem progress update includes any general testing risks and issues encountered that may affect the CSD’s timely completion of User Testing stage. The Contracting CSD reports on its progress against its test plan and reports any risks and issues that may affect its timely completion of the testing stage. When the progress update is shortly before the stage transition, then the Eurosystem uses the progress update as input for User Testing stage transition assessment.

When there is sufficient time remaining before the User Testing stage transition assessment, the Contracting CSD and the Eurosystem assess the need for corrective actions to resolve any identified issues and mitigate any identified risks. Both the Contracting CSD and the Eurosystem determine whether the implementation of the corrective measures is feasible and undertake their respective actions. If there is disagreement of the corrective actions, then the Contracting CSD, the Eurosystem or both can initiate the escalation process.
7.2 User Testing Stage Transition Assessment Process

**User Testing Stage Transition Assessment Process (T2S.UT.S3.020)**

- **PMG Substructure**
  - **PMG**
  - **Eurosystem**
  - **MCR**
  - **CSD/NCB**

- **Disagreement Resolution Process (T2S.PMO.PMF.040)**
  - Review Testing Stage Report and Transition Recommendation
  - Agreement?
    - Yes: Go to next Stage
    - No: Bilateral Escalation Process (T2S.UT.S3.010)

- **Prepare User Testing Stage Report and Recommendation**
- **Send User Testing Stage Report**
- **Assess fulfillment of Entry/Exit Criteria**
- **Is Bilateral Stage?**
  - Yes
    - Review Testing Stage Report and Transition Recommendation
    - Agreement?
      - Yes: Go to next Stage
      - No: Bilateral Escalation Process (T2S.UT.S3.010)
  - No: No

- **Deliver Exit/Entry Documentation**
- **Bilateral Escalation Process (T2S.UT.S3.010)**
- **Send Exit/Entry Documentation**

**Overview:**
- The process begins with the delivery of exit/entry documentation.
- The user testing stage transition assessment process involves reviewing the testing stage report and transition recommendations, assessing fulfillment of criteria, and handling the transition to the next stage.
- Disagreement is handled through a resolution process.
- If the bilateral stage is not agreed upon, the process progresses through bilateral escalation.
- The final step involves delivering exit/entry documentation.
### 7.2.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSD / CB</td>
<td>In this process, the CSD is responsible for:</td>
</tr>
<tr>
<td></td>
<td>▪ Providing a sufficient level of documentation to the Eurosystem to allow the Eurosystem to assess the Contracting CSD’s fulfilment of the entry and exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>▪ Carrying out an assessment of its own fulfilment of the entry and exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>▪ Assessing the proposed correction actions from the bilateral escalation process.</td>
</tr>
<tr>
<td>Eurosystem</td>
<td>In this process, the Eurosystem is responsible for:</td>
</tr>
<tr>
<td></td>
<td>▪ Delivering the documentation to the CSD to allow the CSD to assess the Eurosystem’s fulfilment of the entry / exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>▪ Carrying out an assessment of the its own fulfilment of the entry or exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>▪ Assessing the proposed corrective actions; and</td>
</tr>
<tr>
<td></td>
<td>▪ Drafting, agreeing and finalising the User Testing stage transition assessment report.</td>
</tr>
<tr>
<td>Monitoring of Client Readiness (MCR)</td>
<td>In this process, the MCR has the obligation to:</td>
</tr>
<tr>
<td></td>
<td>▪ Monitor the Contracting CSD’s progress in order to determine whether it has fulfilled the entry or exit criteria for a testing stage;</td>
</tr>
<tr>
<td></td>
<td>▪ Propose and discuss corrective actions in case of non fulfilment of either the exit or entry criteria for a User Testing Stage; and</td>
</tr>
<tr>
<td></td>
<td>▪ Provide guidance to the PMG substructure when required in the case of multilateral escalation.</td>
</tr>
<tr>
<td>PMG substructure</td>
<td>In this process, the PMG substructure is responsible for:</td>
</tr>
<tr>
<td></td>
<td>▪ Discussing the stage transition assessment report and any recommendations;</td>
</tr>
<tr>
<td></td>
<td>▪ Providing the final decision during PMG substructure sessions to go forward to the next stage or into multilateral escalation in case of disagreement.</td>
</tr>
<tr>
<td>Project Managers Group (PMG)</td>
<td>In this process, the PMG is responsible for resolving any potential disagreement on the decision to go forward to the next stage or to initiate the disagreement resolution process.</td>
</tr>
</tbody>
</table>
7.2.2 Process Description

The assessment process for User Testing stage transition defines the steps in assessing and reporting on whether the Eurosystem, CSDs and CBs are prepared to transition jointly from one stage of User Testing to the next based on the exit criteria of the current stage and/or the entry criteria of the next stage.

The Eurosystem provides to the Contracting CSD the templates based on which the Contracting CSD assesses its fulfilment of the exit criteria of the current stage of User Testing or/and the entry criteria for the next stage of User Testing. The Contracting CSD assesses its fulfilment of the exit and/or entry criteria for User Testing stages. The Contracting CSD and the Eurosystem jointly review this assessment as part of the monitoring of client readiness to determine whether the Contracting CSDs has fulfilled the applicable exit and/or entry criteria. Should an exit or entry criteria remain unmet, then the Contracting CSD and the Eurosystem identify and assess corrective actions on the part of the Contracting CSD, the Eurosystem or both parties, depending on the source and required resolution of the issue.

The Eurosystem prepares the User Testing stage transition assessment report that documents whether the Contracting CSDs of a migration wave have fulfilled the exit criteria of the current stage of User Testing or/and the entry criteria for the next stage of User Testing. It documents recommendations for corrective actions should exit or entry criteria remain unfulfilled.

If the User Testing stage transition is bilateral, then the Eurosystem provides the report to the Contracting CSD for assessment and both parties agree in the MCR whether there is a need to report risks and issues multilaterally. If the Contracting CSD and the Eurosystem agree on the reports conclusions for a stage transition, then the Contracting CSD formally enters the next testing stage. If no stage transition is possible or disagreements remain, then the MCR escalates the disagreement as defined in section 7.3 on the bilateral escalation process.

If the User Testing Stage transition is Multilateral, then the Eurosystem provides the report to the PMG substructure. If the ‘PMG substructure agrees on the reports conclusions for a stage transitions, then the Contracting CSDs of a migration wave formally enter the next testing stage as a whole. If not stage transition is possible or disagreements remain, then the PMG substructure escalates the disagreement to the PMG. The PMG is responsible for resolving the potential disagreement on the decision to go forward to the next stage of User Testing. If it cannot reach an agreement, then it initiates as covered by the disagreement resolution process as described in Schedule 2 (T2S Programme Planning and Monitoring).
7.3 User Testing Stage Transition Bilateral Escalation Process

User Stage Transition Bilateral Escalation Process (T2S.UT.S3.010)

Steering Level Bodies

<table>
<thead>
<tr>
<th>T2S Board</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joint Discussion</td>
</tr>
<tr>
<td>Decide on Corrective Actions</td>
</tr>
<tr>
<td>Agreement?</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Impacts other CSDs?</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CSD/NCB Sponsor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare Bilateral Escalation</td>
</tr>
<tr>
<td>MCR</td>
</tr>
<tr>
<td>Prepare Bilateral Escalation</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Back to Triggering Process (Cfr Stage Transition Process) (T2S.UT.S3.020)</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PMG Substructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multilateral Discussion (Cfr Disagreement Resolution Process) (T2S.PMO.PMF.040)</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>
7.3.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>T2S Board</td>
<td>In this process, the T2S Board has the responsibility to discuss the escalated issue and attempt to find a resolution with the CSD / CB sponsor.</td>
</tr>
<tr>
<td>CSD/CB Sponsor</td>
<td>In this process, the CSD/CB sponsor has the responsibility to discuss the escalated issue and attempt to find a resolution with the T2S Board.</td>
</tr>
<tr>
<td>Monitoring of Client Readiness (MCR)</td>
<td>In this process, the MCR prepares the bilateral escalation for the T2S Board and the CSD/CB sponsor.</td>
</tr>
<tr>
<td>PMG substructure</td>
<td>The PMG substructure is responsible for discussing and proposing solutions for a bilateral issue that affects multiple T2S Stakeholders and the successful delivery of T2S.</td>
</tr>
</tbody>
</table>

7.3.2 Process Description

The objective of this process is to resolve bilateral disagreements between the Eurosystem and the Contracting CSD in the User Testing execution phase. An example of such a disagreement would be diverging assessments on whether the Contracting CSD has fulfilled the entry or exit criteria for a specific stage of User Testing. The monitoring of client readiness identifies and raises any issues on User Testing that it cannot resolve to the Contracting CSD’s sponsor and the T2S Board. At Steering Level, the Contracting CSD’s sponsor and the T2S Board will attempt to resolve these disagreements with the objective to avoid entering the disagreement resolution process of Schedule 2 (T2S Programme Planning and Monitoring).

The Steering Level will attempt to resolve the disagreement in a timely manner, taking into account the urgency and the severity of the matter. If the Steering Level has achieved agreement on the disputed issues and the proposed resolution does not affect other T2S Stakeholders, then it submits its resolution to the Contracting CSD and the Eurosystem representatives in MCR for implementation. If the Steering Level has achieved agreement on the disputed issues and the proposed resolution affects other T2S Stakeholders, then it submits its resolution to the PMG substructure for review and a recommendation on its implementation. If ultimately the Steering Level cannot reach an agreement on the resolution of an issue, then it can escalate the issue according to the disagreement resolution process of Schedule 2 (T2S Programme Planning and Monitoring).
7.4 User Testing Suspension Process

User Testing Suspension Process (T2S.UT.S3.030)

- **PMG**
  - Need for suspension identified → Request Suspension
  - Provide guidance
  - Assessment
  - Agreement?
    - Yes: Act Suspension
    - No: Need for suspension identified

- **PMG Substructure**
  - Need for suspension identified → Request Suspension
  - Analyse Reasons & Propose Corrective actions
  - Bilateral Phase?
    - Yes: Assessment
    - No: Plan Impact?
      - Yes: Programme plan Preparation and Assessment Process (T2S.PMO.PMF.000)
      - No: Need for suspension identified

- **Eurosysten**
  - Need for suspension identified → Request Suspension
  - Analyse Reasons & Propose Corrective actions
  - Bilateral Phase?
    - Yes: Assessment
    - No: Plan Impact?
      - Yes: Programme plan Preparation and Assessment Process (T2S.PMO.PMF.000)
      - No: Need for suspension identified

- **MCR**
  - Need for suspension identified → Request Suspension
  - Assess Impact
  - Multilateral Phase?
    - Yes: Assessment
    - No: Plan Impact?
      - Yes: Programme plan Preparation and Assessment Process (T2S.PMO.PMF.000)
      - No: Need for suspension identified

- **CSD/NCB**
  - Need for suspension identified → Request Suspension
  - Bilateral Phase?
    - Yes: Assessment
    - No: Plan Impact?
      - Yes: Programme plan Preparation and Assessment Process (T2S.PMO.PMF.000)
      - No: Need for suspension identified
### 7.4.1 Process Actors and their Roles

<table>
<thead>
<tr>
<th>Process Actor</th>
<th>Process Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSD / CB</td>
<td>The CSD or CB is responsible for identifying the need to and issuing the request to suspend User Testing.</td>
</tr>
<tr>
<td>Eurosystem</td>
<td>The Eurosystem has the responsibility for:</td>
</tr>
<tr>
<td></td>
<td>• Analysing the CSD or CB request to suspend User Testing;</td>
</tr>
<tr>
<td></td>
<td>• Proposing corrective measures to avoid a suspension of User Testing;  and</td>
</tr>
<tr>
<td></td>
<td>• Preparing the assessment of and a recommendation on the suspension request.</td>
</tr>
<tr>
<td>Monitoring of Client Readiness (MCR)</td>
<td>In this process, the MCR depicts the bilateral steps of this process for:</td>
</tr>
<tr>
<td></td>
<td>• Reviewing and discussing the status of User Testing;  and</td>
</tr>
<tr>
<td></td>
<td>• Assessing the status of User Testing and providing guidance to the PMG substructure when required in the case of multilateral escalation.</td>
</tr>
<tr>
<td>PMG substructure</td>
<td>In this process, the PMG substructure is responsible for:</td>
</tr>
<tr>
<td></td>
<td>• Discussing the stage transition assessment report and any recommendations;  and</td>
</tr>
<tr>
<td></td>
<td>• Providing the final decision during PMG substructure sessions to go forward to the next stage or into multilateral escalation in case of disagreement.</td>
</tr>
<tr>
<td>Project Managers Group (PMG)</td>
<td>The PMG provides guidance to the PMG substructure in order to resolve disagreements on the potential suspension of User Testing. If the PMG substructure cannot reach an agreement, then the PMG is responsible for resolving any potential disagreement on the decision to suspend or for initiating the disagreement resolution process.</td>
</tr>
</tbody>
</table>

### 7.4.2 Process Description

This process describes the steps in taking a decision on a request from a Participating CSD or a Central Bank to suspend the current stage of User Testing. Participating CSDs/CBs individually or the PMG substructure may identify the need to suspend User Testing, e.g. too many unresolved defects of various severities to allow the continuation of proper testing. The individual Participating CSD/CB or the PMG substructure submits the request with its business justification to suspend User Testing to the Eurosystem.

The Eurosystem analyses the suspension request and, when possible to avoid the suspension to User Testing, proposes corrective action:

- To the individual Participating CSD/CB that initiated the request when the request is bilateral; and
- To the PMG substructure when it initiated the request as a bilateral request.
When the suspension request is bilateral, then:

- the Participating CSD/CB jointly reviews the Eurosystem assessment of the suspension request in MCR; and

- the Participating CSD/CB and/or Eurosystem implement(s) any identified corrective actions to limit and/or avoid a suspension of User Testing.

If the suspension of User Testing is unavoidable and has no planning impact, then the MCR may initiate the suspension. If the suspension of User Testing is unavoidable and has a planning impact, then the MCR initiates an assessment of the planning impact that follows the programme plan preparation and assessment process in Schedule 2 (T2S Programme Planning and Monitoring).

When the suspension request is multilateral or the bilateral request has a multilateral impact, then the Eurosystem prepares the assessment and recommendation for the assessment in the PMG substructure. The PMG substructure may request guidance from the PMG to facilitate a decision on the potential suspension of User Testing. In the case that the PMG substructure cannot reach an agreement, it may revert to the PMG to reach an agreement. If the PMG substructure cannot reach an agreement on the decision to suspend, then it initiates the disagreement resolution process as defined by the disagreement resolution process defined in Schedule 2 (T2S Programme Planning and Monitoring).

If the PMG substructure or the PMG reaches an agreement on the request and the request has no planning impact, then the PMG substructure may initiate the suspension. If the suspension of User Testing is unavoidable and has a planning impact, then the PMG substructure initiates an assessment of the planning impact that follows the programme plan preparation and assessment process in Schedule 2 (T2S Programme Planning and Monitoring).
7.5 Release Management during the User Testing

The Release Management Process applicable to test environments and originating from defect resolutions during the User Testing execution phase and during the testing of the subsequent T2S releases (as defined in Chapter 5 of Schedule 9) is in the remit of the PMG substructure ensuring that all technical and non-technical aspects are considered together.

7.6 Supporting Processes - IT Service Management Processes

As described in chapter 3.1 it is the Eurosystem’s responsibility to establish and operate the necessary IT service management processes that includes a defect resolution to remedy errors based on the principles of ITIL V3 Service Operation.

The PMG substructure will detail these IT service management processes such as the defect resolution and incident handling applicable to test environments following as much as possible and where relevant the principles laid down in the Manual of Operational Procedures (MOP). Furthermore, the definitions of the severity of defect and the incident resolution times applicable during User Testing are defined in Schedule 6 (T2S Service Level Agreement).
8 Post-Migration Testing

Post-migration testing shall refer to all testing activities of CSDs, CBs and Directly Connected Parties (DCPs) after go-live of the final migration wave for the initial release of T2S. Events, such as the migration of a new CSD / CB to T2S or the implementation of a new release, will require post-migration testing.

The following principles shall apply for post-migration testing:

- The Project Managers Group (PMG) shall perform an impact assessment for a new T2S release or a new CB/CSD joining T2S on the T2S Actors in order to determine whether all T2S Actors will need to carry out User Testing for the T2S release or whether only affected T2S Actors need to test.

- Based on the impact assessment, the Project Managers Group (PMG) with the support of the PMG substructure on User Testing shall propose a post-migration test plan to the Steering Level for approval.

- The post-migration test plan must ensure that CSDs, CBs and DCPs will have sufficient time to verify that the delivered T2S functionality meets the agreed requirements and specifications as defined in the T2S Scope Defining Set of Documents.

- Post-migration testing shall use the framework as defined in this Schedule.

- The PMG in their impact assessment will make a recommendation to the Steering Level on whether the introduction of the new T2S release will require the re-certification of CSDs and/or CBs. The T2S Board shall take the final decision on whether CSDs and/or CBs must recertify themselves for a new release of T2S.
Annex 1 - Mapping of testing activities on the test environments

In accordance with the principles for sharing testing facilities, the Eurosystem will not plan any 
Eurosystem Acceptance Testing activity on the testing environments used for User Testing.
The following diagram presents the mapping of the testing activities for each migration wave on 
the test environments.
Framework Agreement

Schedule 3 – Annex 1 – Mapping of testing activities on the test environments

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Eurosystem Acceptance Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pilot Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity Set-up &amp; Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 1 Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSD Acceptance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 2 Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSD Acceptance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 3 Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSD Acceptance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 4 Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSD Acceptance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remedy period in accordance with Article 38(1)(b) of the FA

Overlap of Wave II and Wave III Multilateral Interoperability testing stage

884
Framework Agreement

Schedule 3 – Annex 1 – Mapping of testing activities on the test environments

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity Set-up &amp; Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slow Motion Bilateral Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSD Acceptance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 2 Migration Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 3 Migration Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 4 Migration Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity Set-up &amp; Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE I Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Migration Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community/Busine Day</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 2 Community/Busine Day</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 3 Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community/Busine Day/Stabilisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 4 Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community/Busine Day/Stabilisation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Community</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-Prod</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity Set-up &amp; Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pre-Production tests</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WAVE 2 – Community - Cycle 2*</td>
<td>01 Aug 30 Sep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Wave 1 Go-Live</td>
</tr>
<tr>
<td>Phased-in connectivity set-up and connectivity testing for waves 2, 3 &amp; 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Wave 2 Go-Live</td>
</tr>
<tr>
<td>Wave 3 Go-Live</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wave 4 Go-Live</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* With Liquidity Transfer Utility

885

31 October 2011

Page 3 of 3
FRAMEWORK AGREEMENT

SCHEDULE 4
MIGRATION
1 Introduction

This document aims at presenting the provisions related to the framework that will be used to prepare and conduct the migration to T2S of the Contracting CSD, Participating CSDs and their communities, as well as the roles and responsibilities of the contracting parties along the migration process from the preparation phase until the end of the Migration Period.

The document is divided into six chapters, corresponding to the major aspects identified as relevant for the migration framework: i) objective and scope of the Migration Schedule; ii) general responsibilities of the contracting parties; iii) composition of the migration waves; iv) preparation of the migration; v) implementation of the migration and vi) post-migration and closing activities (e.g. reporting on lessons learned, updates of the configuration parameters upfront each migration wave in order to ensure the cross-CSD settlement with the new migrating CSDs).
12 **Objective and scope of the Migration Schedule**

2.1 **Objective**

The objective of the T2S migration is to enable a smooth and successful transition to the usage of the T2S Services for the Contracting CSD, Participating CSDs and their communities once the prerequisites for their migration are fulfilled. As stated in the User Requirements Document, “Migration in the context of T2S means the relocation of data from a CSD to the T2S infrastructure and the associated changes in the processes and technical environment of a CSD on a mutually agreed date”. This covers also the associated changes to the configuration items of a CSD.

2.2 **Scope**

In terms of activities, the scope of this Migration Schedule covers all activities that are related to the preparation of the T2S production environment for the successful migration of a Contracting CSD, the Participating CSDs and their communities. Chapter 5, 6 and 7 provide the relevant information concerning the migration related activities. Although the migration process is interrelated with other processes, in particular the User Testing until the end of Migration Period, the T2S Programme Plan and the Release Management during the Migration Period (if releases/ software updates are envisaged during this period), such other activities will be described separately in the relevant Schedules.

With regards to the users, in the context of the Framework Agreement the T2S migration perimeter consists of all CSDs that have entered into a contractual relationship with the Eurosystem for the use of T2S in view of their connection to T2S during the Migration Period. Other CSDs fall outside this migration perimeter. Whenever relevant, references will be made to coordination of migration activities with other T2S Actors, but the actual provisions applicable to those T2S Actors will be covered as part of the legal relationship with these T2S Actors.
3 General responsibilities of the Contracting Parties

As an overarching principle, the Eurosystem and the Contracting CSD shall cooperate in good faith for the preparation and execution of all T2S migration activities.

3.1 General responsibilities of the Eurosystem

In view of preparing and ensuring a successful migration to T2S of the Contracting CSD, the Participating CSDs and their communities, the Eurosystem shall:

a) cooperate in good faith with the Contracting CSD and the other T2S Actors and provide them with all relevant information to prepare the necessary procedures and processes for all migration activities and related deliverables, identified in Schedule 2 (T2S Programme Planning and Monitoring);

b) coordinate, steer and monitor the T2S migration process. In agreement with the Contracting CSD and the Participating CSDs, it establishes the migration plan, the tasks and the milestones for the migration process and monitors compliance with the agreed procedures and milestones;

c) prepare the life-cycle of the migration process which consists of three phases: (i) the planning phase, which consists of activities related to the preparation of the migration activities that need to be planned in advance in order to mitigate the migration risks; (ii) the implementation phase, which consists of the actual preparations for live operations and (iii) the closing phase, which consists of closing reports aiming at improving the next migration based on lessons learned from the initial migration. The diagram outlining the sequence and interrelations of the migration activities, as well as the milestones of the T2S migration phases are presented in Annex 1 (Migration milestones) to this Schedule;

d) set up a PMG substructure, which will be in charge of coordinating, supporting and monitoring the work related to the migration activities, in accordance with the T2S Governance and the provisions set out in section 3.3 of this Schedule;
e) nominate one person for each Contracting CSD and Participating CSDs as migration correspondent for that CSD, as well as a T2S migration coordinator in charge of monitoring and coordinating all activities to be carried out during the migration process;

f) ensure the readiness of the T2S production environment according to the provisions of Schedule 2 (T2S Programme Planning and Monitoring) in order to enable the Contracting CSD to plan and carry out all activities on the T2S production environment required for its migration to T2S;

g) ensure the readiness of T2S for all migration waves, meaning that the enhancements to the system are reduced to the resolution of blocking and severe defects discovered during the Migration Period;

h) ensure the readiness of the Dedicated Cash Accounts in euro, prior to the T2S Go-Live Date, upon the request of Dedicated Cash Account holders in accordance with the rules and conditions set up by the respective euro area NCB;

i) provide all reasonable support to non-euro area NCBs in ensuring the readiness of Dedicated Cash Accounts in their currency, prior to the first settlement of securities transactions in their currencies by a CSD located in the country of the non-euro area NCB. The opening of these Dedicated Cash Accounts will be driven by the request of the Dedicated Cash Account holders in accordance with the rules and conditions set up by the respective non-euro area NCB;

j) upload and maintain the necessary Common Static Data and system configuration parameters sufficiently in advance of the migration of the Contracting CSD. The Common Static Data will be created upfront with a future “valid from” date;

k) provide support to the Contracting CSD and the Participating CSDs – in particular in accordance with section 21.8 (Data migration tools) of the URD – for the transfer of:

   i. the Common Static Data as required, typically three months before the migration of the first Investor CSD to T2S, which requires such data, and;

   ii. its CSD Static Data and Dynamic Data prior to its migration to T2S;

l) ensure that the collateral management function for the Eurosystem credit operations is provided as of the start of securities transaction settlement in T2S;
m) report progress on the overall migration process on a regular basis and share relevant information with the Contracting CSD and the Participating CSDs on their level of readiness (based on information provided by those);

n) apply an escalation and decision-making process in accordance with the general T2S governance arrangements, as specified in Schedule 8 (Governance);

o) provide support to the Contracting CSD and the Participating CSDs with regard to their migration activities, including during the process of “de-migration” of the Contracting CSD in case the Contracting CSD faces severe problems due to significantly degraded Service Level during the week after its migration to T2S;

p) provide training sessions for the migration to the Contracting CSD and the Participating CSDs and all necessary support to facilitate the training sessions provided by the Contracting CSD or the Participating CSDs to their communities;

q) commit to keep the Migration Period as short as possible in order to limit adverse competition effects between migrated CSDs and non-migrated CSDs;

r) aim to ensure a level playing field between the Contracting CSD and the Participating CSDs that migrate earlier or later, including but not limited to the provision of specific functionality following the provisions of the Change and Release Management, as specified in Schedule 9 (Change and Release Management).

3.2 General responsibilities of the Contracting CSD

In view of preparing and ensuring a successful migration to T2S, the Contracting CSD shall:

a) cooperate in good faith with the Eurosystem and with other relevant T2S Actors and provide all relevant information to prepare the necessary procedures and processes for all migration activities and related deliverables, identified in Schedule 2 (T2S Programme Planning and Monitoring);

b) determine, in cooperation with the Participating CSDs, the migration wave in which it shall migrate to T2S and the date of its migration in accordance to the criteria and the process specified in sections 4.2 and 4.3 of this Schedule and within the time stipulated in Schedule 2 (T2S Programme Planning and Monitoring);
c) migrate to T2S by the committed date which will be defined in accordance with the process as specified in the section 4.3. of this Schedule;

d) ensure its own readiness for the migration to T2S by the committed date according to the procedures and processes agreed with the Eurosystem and other T2S Actors;

e) take all necessary measures to facilitate the readiness of its community for the migration to T2S by the agreed date according to the procedures and processes agreed with the Eurosystem and other T2S Actors;

f) set up its own migration project, define its migration plan, allocate appropriate resources to the implementation of such a plan, as well as assess and adjust such migration plan and the allocated resources, where necessary, with a view to ensuring a smooth migration to T2S according to the agreed plan; the adjustments to migration plans must be discussed and agreed with the Eurosystem and other T2S Actors as changes may have an impact on all the involved parties;

g) be involved in the decision to go-live, independently of its migration wave; in particular by indicating whether or not the exit criteria for the business day testing are fulfilled and on the level of comfort that all remaining blocking and severe defects will be solved in time in order to avoid any impediments for the later migrating CSDs;

h) upload and maintain the Common Static Data as required, (e.g. all the Securities Reference Data for which the Contracting CSD is responsible according to the agreed mechanism for assigning responsibility in the maintenance of Securities Reference Data), typically with three months before the migration of its first Investor CSD, irrespective of the migration wave where the Contracting CSD is envisaged to join T2S;

i) upload and maintain its CSD Static Data and Dynamic Data prior to its migration to T2S; these data will be created upfront with a future “valid from” date;

j) maintain all the necessary links with the Participating CSDs until the end of the Migration Period in accordance with the provisions agreed between the Contracting CSD and Participating CSDs;

k) provide training sessions to its community sufficiently in advance of community testing;
Schedule 4 – Migration

1) report progress on its readiness for migration according to the agreed procedures, frequency and level of detail, with a particular view to identifying developments that might jeopardise the migration of the Contracting CSD according to the agreed plan;

m) nominate one person for coordinating all migration activities within its own organisation and ensure that such person shall duly and regularly participate in the meetings organised by the Eurosystem until the Contracting CSD has migrated to T2S, and, in particular where this is not practicable, in the written procedures;

n) mitigate the risk that a member of the Contracting CSD’s community would impede the migration of that CSD and the rest of its community, by limiting the dependencies between the Contracting CSD and its community as much as possible. In particular, keeping an indirect connection should be envisaged as contingency when the connectivity for a User wishing to connect directly does not work properly at the moment of the migration.

3.3 Cooperation and escalation procedures

The Eurosystem shall apply an escalation and decision-making process for communication in accordance with the general T2S governance arrangements, as specified in Schedule 8 (Governance).

The Eurosystem shall set up a PMG substructure, in accordance with the T2S governance, for the coordination and monitoring of the migration activities. This substructure shall meet on a regular basis and shall at least be composed of the ECB migration coordinator, the 4CB migration coordinator, and a migration coordinator from each CSD (as mentioned in section 3.2 m) of this Schedule).

The role of the substructure in charge of migration shall be to:

- Coordinate and review migration activities;
- Monitor the implementation of the migration plans;
- Agree with the Contracting CSD a tailored migration plan;
- Discuss issues raised by the members of the substructure and try to resolve disagreements;
Communicate with the T2S Programme management office on the planning of migration activities;

Prepare communications related to migration to the various T2S Stakeholders and the public at large.

In case of an issue requiring immediate action, the following process shall be followed:

- The Contracting CSD shall request a conference call with the Eurosystem during the next business day or at its earliest convenience;
- The issue shall be discussed during the conference call;
- The Eurosystem shall summarize the outcome of the conference call and distribute it to the members of the substructure in charge of migration.

The substructure in charge of migration shall convene at its earliest convenience to:

- Assess the nature of the issue;
- Assess the impact of the issue on the various T2S Actors;
- Assess any potential impact on the organisation and the timing of the migration activities for the various T2S Actors;
- Prepare an action plan, and the necessary communication, if any, to address the issue.

In case no agreement can be reached in the substructure, each party shall be entitled to escalate the problem to the Project Managers Group (PMG), where the situation shall be discussed and rapidly assessed.

If a mutually agreeable solution cannot be found in the PMG, then the disagreement resolution process shall apply as described in Schedule 2 (T2S Programme Planning and Monitoring) whereby the issue is escalated to the Steering Level in order to receive guidance to resolve the issue.

Ultimately there shall be recourse to the dispute resolution process as described in Article 42 of the Framework Agreement.
4 Composition of the migration waves

4.1 General migration approach

The migration to T2S will follow a phased approach and will be organised to reach the following objectives:

- give the necessary flexibility for the planning and coordination of the migration activities;
- allow for a gradual build-up of volumes;
- mitigate the risk that the Contracting CSD or any of the Participating CSDs fail to successfully migrate to T2S on the agreed date, thereby avoiding interruptions in the Contracting CSD’s business;
- ensure system stability from a functional and technical perspective throughout the migration process.

This phased approach will be implemented via a migration “by CSD” approach, which allows the Contracting CSD, the Participating CSDs and their communities to migrate to T2S in different waves and on different pre-defined dates.

The migration will be organised in 4 migration waves, with a minimum period of 21 weeks between each wave. In addition, a contingency migration wave is available (not later than 6 months after the date of the last migration wave), to be used in case the Contracting CSD cannot migrate as originally committed. The Contracting CSD and the Participating CSDs participating in the first wave will preferably bring at least one Directly Connected Party to T2S.

The migration of the Contracting CSD will take place during a weekend and will be driven by settlement date. The migration to T2S will not take place on a “sensitive” weekend during critical periods for CSDs and Central Banks such as corporate actions season, freeze periods or periods of significant market stress, etc.

4.2 Criteria for defining the composition of migration waves
As an objective, the following criteria should be fulfilled for defining the composition of the migration waves:

### 4.2.1 Criteria applicable to the first migration wave (migration wave 1)

**Criterion 1: Functional stabilisation**

The number of transactions, to be migrated with the first wave should not be less than 10% or more than 40% of the expected normal volume of transactions, aiming to ensure functional stabilisation with a limited business and operational risk.

**Criterion 2: Functional coverage**

The functionalities of the T2S Platform\(^1\) should be covered as much as possible by the first migrating CSDs.

### 4.2.2 Criterion applicable to the second and the subsequent migration waves

In order to address the risk of performance issues and to ensure that the anticipated T2S capacity will be sufficient to cope with the normal (and peak) volumes per each wave, some measures may be required to be taken to fulfil the SLA on the T2S production environment, including a fine-tuning of the performance of the system from one wave to the next wave.

**Criterion 3: Fine-tuning the performance of the system**

As an objective, the number of transactions to be migrated in the second wave and in each subsequent migration wave should not exceed 50% \(^2\) of the expected normal number of transactions.

---

\(^1\) Including those related to non-euro settlement currencies, unless the related risks cannot be managed or accepted.

\(^2\) The 50% limit is the maximum volume per each migration wave and not the accumulated volume of a particular migration wave and the volume of the preceding wave(s) or the future wave.
4.2.3 Criteria applicable to all migration waves

Criterion 4: Readiness of internal system

The Contracting CSD should ensure the readiness of its internal applications – as well as its technical and operational preparations – in order to be able to perform and complete its migration related activities.

Criterion 5: Certification requirements

The Contracting CSD, together with its community, should make all endeavours to successfully pass the certification tests, as described in Schedule 2 (T2S Programme Planning and Monitoring) and Schedule 3 (User Testing).

Criterion 6: Structural links

The structural links between the Contracting CSD and the Participating CSDs should be taken into consideration in the migration wave composition based on the preference expressed by the Contracting CSD with whom they would like to migrate in the same wave. In addition, the volume of the transactions settled via the cross-border links will be taken into account (i.e. the more transactions are settled via the links between the CSDs that have preferred the same migration wave, the more this will be considered as justification to be grouped in the same migration wave).

4.3 Process for defining the composition of migration waves

Without prejudice to the right of the Contracting CSD to request the Eurosystem directly to be able to migrate in wave 1, the process envisaged for the composition of the migration waves and the respective migration dates will be determined as follows:

1. The Contracting CSD and the Participating CSDs will prepare a proposal by synchronisation point 2 – (Feasibility Confirmation by CSD/CB) as defined in Schedule 2 (T2S Programme Planning and Monitoring) for the dates of the migration waves (excluding the T2S Go-Live Date and contingency wave date) and the allocation of individual CSDs to the migration waves, in accordance with the criteria and conditions specified in this Schedule and within the time stipulated in Schedule 2 (T2S Programme Planning and Monitoring).
2. The Eurosystem will consider the proposal expressed by the Contracting CSD and the Participating CSDs against the criteria and conditions specified in this Schedule and within the time stipulated in Schedule 2 (T2S Programme Planning and Monitoring).

3. If the composition and dates of the migration waves, based on the proposal made by the Contracting CSD and the Participating CSDs meet the criteria and conditions specified in this Schedule and are within the time stipulated in Schedule 2 (T2S Programme Planning and Monitoring), the Eurosystem will inform the Contracting CSD and each of the Participating CSDs accordingly, who will commit to its preferred migration date.

4. If the Contracting CSD and the Participating CSDs do not come with a proposal by synchronisation point 2 – (Feasibility Confirmation by CSD/CB) as defined in Schedule 2 (T2S Programme Planning and Monitoring) or the proposal made by the Contracting CSD and the Participating CSDs for the composition and dates of the migration waves does not meet the criteria and conditions specified in this Schedule and Schedule 2 (T2S Programme Planning and Monitoring), the Contracting CSD and/or other Participating CSDs may be allocated to another migration wave, after thorough consideration of the options by the PMG, in particular taking into account the consequences of such reallocation for the affected Contracting CSD and/or Participating CSDs. The PMG will submit its proposal/recommendation to the Steering Level for decision. In preparing its proposal, the substructure shall take into consideration any potential detrimental and material impact on the Contracting CSD which is asked to move to another migration wave than its preferred one.

5. When the available means to resolve the issue have been exhausted, in particular the dispute resolution and escalation possibilities laid down in Article 42 of the Framework Agreement, the Eurosystem may decide on the migration date, provided that such date is not earlier than the one indicated by the Contracting CSD as its preferred date and provided further that the Contracting CSD has not indicated a preferred date.

6. Once the composition and dates of the migration waves have been defined and agreed by the contracting parties, this Schedule and Annex will be amended pursuant to the amendment rules defined in Article 47 of the Framework Agreement.
5 Preparation of the migration

The activities to be carried out for the preparation of the T2S Go-Live Date and the migration of a Contracting CSD and its community need to be well planned in advance in order to mitigate the risks related to the migration process.

5.1 Responsibilities of the Eurosystem

In order to prepare and organise the migration related activities, the Eurosystem – in cooperation with the Contracting CSD – shall:

a) set up a bilateral coordination structure between the Eurosystem and the Contracting CSD in addition to the multilateral coordination which the PMG will ensure;

b) establish the standard migration plan for all Participating CSDs and the Contracting CSD that will join T2S, including aspects related to the set-up of Securities Accounts and accounts structures, set-up of Dedicated Cash Accounts, major project milestones, the necessary Dynamic Data to be input into the system, as well as checkpoints to be met before the start of the migration weekend;

c) agree with the Contracting CSD in establishing the tailored migration plan per Contracting CSD or group of Participating CSDs depending on its specificities;

d) establish the detailed migration weekend script for each migration wave which provides the Contracting CSD with the required information to execute the tasks and/or to carry out the actions required during the migration weekend;

e) establish the fall-back arrangements and roll-back procedures specific for each migration wave, in order to manage the necessary processes if the migration needs to be deferred to a later stage due to predictable or unforeseen circumstances, and/or if the activities already performed during the migration weekend need to be unwound if the migration has to be stopped;
f) provide support to the Contracting CSD – in particular in accordance with section 21.8 (Data migration tools) of the URD – if it has been demonstrated, following the applicable crisis management arrangements, that there is a need to “de-migrate” to its legacy system immediately after its migration in case the Contracting CSD faces severe problems at that time, either due to significantly degraded Service Levels, or because of severe problems at the Contracting CSD itself;

g) define the registration guide/procedures in order to enable the Contracting CSD to describe in detail their participation data, services used and account usage details;

h) establish the structure and elements of the migration profile for each Contracting CSD which gives a structured overview of the set-up of CSDs on their first day of operation in T2S;

i) define the necessary Common and CSD Static Data and Dynamic Data to be uploaded in the system, as well as the relevant message formats;

j) re-plan and reschedule certain migration activities as required, based on a strong coordination and decision-making process between the Eurosystem and the Contracting CSD and Participating CSDs, in the eventuality that an unexpected event (within and out of the control of the CSD) will impede the migration of one or more Participating CSDs on the scheduled date;

k) actively monitor throughout the migration process the level of the Contracting CSD’s preparedness;

l) prepare progress reports to the appropriate bodies on the status of each Contracting CSD based on the information provided by the Contracting CSD and the Participating CSDs according to pre-agreed dashboard indicators;

m) establish the communication framework for the migration process which covers the information exchanged with the Contracting CSD and the Participating CSDs and the market about the migration process and about individual migrations. Communications will be prepared jointly by the Eurosystem and the Contracting CSD and the Participating CSDs, in accordance with the provisions of the Framework Agreement and section 3.3 of this Schedule;
n) establish specific operational procedure and rules, if needed, to be followed by the Contracting CSD during the Migration Period where some Participating CSDs will operate under the new operational regime of T2S, while the non-migrated Participating CSDs are still operating according to the current regime.

5.2 Responsibilities of the Contracting CSD

In order to prepare and organise the migration related activities, the Contracting CSD – in cooperation with the Eurosystem - shall:

a) organise, prepare and monitor its own migration process and take appropriate measures in order to ensure its own readiness for joining T2S;

b) monitor and take all necessary measures to facilitate the readiness of its community for the migration to T2S;

c) cooperate with the Eurosystem in preparation of the standard migration plan and the detailed migration weekend script;

d) agree with the Eurosystem in establishing a tailored migration plan (including a fall-back plan) based on the standard migration plan, and specify the type of support and tools, if any, that are considered necessary to facilitate the activities meant in section 5.1 f) of this Schedule;

e) coordinate the readiness of its community for migration to T2S. The Contracting CSD shall take all necessary measures to facilitate the readiness of the Securities Accounts of its participants in T2S i.e. the creation and availability of Securities Accounts;

f) shall monitor the readiness of Dedicated Cash Accounts on the basis of the confirmation provided by its participants (which the latter obtain from the relevant Central Bank(s)) regarding the creation and availability of Dedicated Cash Accounts in T2S;

g) identify any “critical participants” that might jeopardize the migration of the Contracting CSD and involve them actively in the migration project, monitoring their preparations more closely and possibly envisaging fall-back arrangements to settle their transactions;

h) establish and maintain, if needed, interim procedures for handling the links with the non-
migrated Participating CSDs, until all Participating CSDs have migrated to T2S;

i) decide individually on the timing for the direct connectivity of members of its community (as of the first day of the migration or after a stabilisation period) provided that the date has been communicated and agreed well in advance with the Eurosystem, and without prejudice to the Contracting CSD’s decision to offer direct connectivity or not;

j) communicate the decision on the migration date of the direct connectivity well in advance to its Directly Connected Parties, in order to allow them to organise and plan their migration activities;

k) ensure indirect connectivity for its Directly Connected Parties, in order to avoid any dependency between the migration of the Contracting CSD and its Directly Connected Parties, in particular if some of its Directly Connected Parties are planned to migrate simultaneously.
6 Implementation of the migration

The implementation phase consists of the actual preparations for live operations and the execution of the tasks on the T2S production environment, in particular all activities that need to be carried out from the moment when the Eurosystem has made the T2S production environment available to the Contracting CSD and Participating CSDs until the successful migration of the Contracting CSD.

6.1 Responsibilities of the Eurosystem

Prior to the start of the implementation phase, the Eurosystem shall:

a) confirm the readiness of the T2S production environment, including the system’s compliance with specific non-functional requirements, in particular related to technical performance, business continuity and information;

b) make available to the Contracting CSD the versions of all the functional and operational documentation (e.g. GFS, UDFS, User Handbooks, Manual of Operational Procedures), which are compliant with the T2S production environment and/or will be used for live operations;

c) set up coordination bodies, in accordance with the T2S Governance, for the coordination and monitoring of the activities to be carried out from the moment when the Eurosystem has made the T2S production environment available to the Contracting CSD until the successful migration of the last migrating CSD, as well as for the decision-making in case an incident occurs which might jeopardise the migration to T2S.

During the implementation phase, the Eurosystem shall:

a) carry out all the pre-migration activities and the activities required during the migration weekend, according to the agreed plan;

b) ensure prior to the T2S Go-Live Date that the complete T2S functionality is available in the T2S production environment and all critical and severe defects encountered during the User Testing have been corrected, so as to avoid the implementation of functional releases during the Migration Period;
c) confirm – prior to the start of first migration wave and the subsequent migration waves - the correct functioning of the T2S production environment according to the T2S Scope Defining Set of Documents and other relevant documents, including the successful execution of an inter-region rotation before the first and second migration wave and that the conditions agreed during the previous go/ no-go decision are met;

d) upload and maintain the necessary Common Static Data and configuration data parameters sufficiently in advance of the migration of the Contracting CSD; these data will be created upfront with a future “valid from” date;

e) confirm the start of the activities during the migration weekend and subsequently the successful completion of each migration on the basis of a report prepared in collaboration with the Contracting CSD and the Participating CSDs. The former confirmation will only be given, in particular, if the exit criteria of the User Testing have been successfully completed and a timetable for implementation of the corrections for the remaining severe defects has been mutually agreed with the Contracting CSD and the Participating CSDs;

f) provide support to the Contracting CSD for the transfer of:

   i. the Common Static Data as required, typically three months before the migration of the first Investor CSD which requires such data and;

   ii. its CSD Static Data and Dynamic Data prior to the migration of the Contracting CSD to T2S;

g) report progress on the activities carried out during the implementation phase by the Eurosystem and the Contracting CSD and the Participating CSDs according to the agreed procedures, frequency and level of detail, with a particular view to identifying aspects that might jeopardise the migration according to the agreed plan;

h) provide support to the Contracting CSD and the Participating CSDs to perform the required actions if needed;

i) provide all necessary support to the non-euro area NCBs that have committed to open Dedicated Cash Accounts in T2S, in order to allow the successful migration of the relevant CSD(s) according to plan.
6.2 Responsibilities of the Contracting CSD

Prior to the T2S Go-Live Date, the Contracting CSD shall:

a) obtain the certification from the Eurosystem for the uploading and the maintenance of Common Static Data or CSD Static Data on the T2S production environment as a precondition to start any activities on the T2S production environment;

b) establish and verify its connectivity to the T2S production environment for each of the networks selected by the Contracting CSD;

c) upload and maintain the Common Static Data as required, typically three months before the migration of its first Investor CSD, irrespective of the migration wave where the Contracting CSD is envisaged to join T2S.

Prior to the start of its migration weekend, the Contracting CSD shall:

a) obtain the certification from the Eurosystem for settling securities transactions on T2S;

b) verify and confirm that its internal systems and processes and those of its participants are ready to efficiently interact with T2S;

c) verify and confirm that T2S delivers the expected services as agreed in the T2S Scope Defining Set of Documents, in particular by having obtained the possibility to verify that all critical defects have been solved, including those discovered during the implementation phase;

d) verify the availability of the necessary Dedicated Cash Accounts to be opened by the euro and non-euro area NCBs at the request of the Dedicated Cash Account holders;

e) confirm the validity of the T2S functional and operational documentation;

f) confirm its readiness for migration and that of its community to T2S according to the agreed migration plan;

g) upload and maintain its CSD Static Data as required prior to its migration weekend; these Data will be created upfront with a future “valid from” date;
h) complete all required forms for the registration on the T2S production environment and provide them to the Eurosystem by the agreed time;

i) ensure timely access to relevant Common and CSD Static Data

j) carry out all the required pre-migration activities according to the agreed migration plan.

During the migration weekend, the Contracting CSD shall:

a) carry out all the activities required during the migration weekend according to the agreed migration plan;

b) upload and maintain its Dynamic Data into the T2S production environment;

c) report on the status of the activities carried out during the migration weekend according to the agreed procedures, frequency and level of detail;

d) confirm the end of its migration based on the successful completion of the activities to be carried out during the migration weekend according to the agreed plan.
7 Closing phase

The closing phase covers the final reporting and the assessment of the lessons learned during the migration process.

7.1 Responsibilities of the Eurosystem

During the closing phase, the Eurosystem shall:

a) provide reports on lessons learned from a migration wave to be applied to the next migration waves;

b) ensure the necessary updates and improvements in the migration plans in order to smoothen the next migration waves.

7.2 Responsibilities of the Contracting CSD

During the closing phase, the Contracting CSD shall:

a) provide feedback to the Eurosystem based on its experience gained during its migration in order to improve the migration of the next waves;

b) update the configuration parameters upfront each migration wave in order to ensure the cross-CSD settlement with the forthcoming migrated CSDs;

c) take all necessary measures to support the migration of the non-migrated Participating CSDs.
Annex 1: Migration milestones

**Conceptual Phase**
- Migration strategy
- Generic migration plans

**Planning phase**
- Composition of migration groups
- Migration dates
- Standard and tailored migration plans
- Registration guide
- Fall-back arrangements
- Roll-back procedures
- Training

**Implementation phase**
- Go/no-go decision
- Connectivity tests on PROD
- Registration process
- Static and dynamic data uploading
- Migration on pre-defined dates

**Closing phase**
- Final reporting
- Lessons to be learned

**Phase I**
- T1
- Start of the migration process

**Phase 2**
- T2
- Preparatory work following the strategy

**Phase 3**
- T3
- Go-live T2S

**Phase 4**
- T4
- Migration wave 1

**Migration Period**
- Migration wave 1
- Contingency wave

**Active Stakeholders**
- C1
  - Start preparation for migration
- C2
  - Migration of necessary common static data if an investor CSD migrates in W1
- C3W1…..C3W4 + Contingency wave

**Migration to T2S wave 1…4 + contingency wave, if required**
FRAMEWORK AGREEMENT

SCHEDULE 5

T2S SERVICE DESCRIPTION
Table of contents

1 T2S SERVICE DESCRIPTION OVERVIEW .......................................................... 1
  1.1 PURPOSE OF THIS NOTE .............................................................................. 1
  1.2 SCOPE OF THE T2S SERVICE DESCRIPTION .................................................. 1

  1.2.1 Within the scope of the T2S Service Description ....................................... 1

1.3 OUTSIDE OF THE SCOPE OF THE T2S SERVICE DESCRIPTION .................. 2

1.4 T2S SERVICE DESCRIPTION AND ITS RELATIONSHIP TO OTHER DOCUMENTS 2

2 SERVICE DELIVERY FRAMEWORK ................................................................. 3
  2.1 SCOPE OF T2S INSTRUMENT ......................................................................... 3

  2.2 SCOPE OF T2S INSTRUCTION AND TRANSACTION TYPE ........................... 3

3 T2S SD: OVERVIEW T2S SERVICES ................................................................. 4

4 T2S SD.SETT: SETTLEMENT SERVICES SERVICE CLASS ......................... 6
  4.1 T2S SD.SETT 010: BUSINESS VALIDATION SERVICE .................................. 6

  4.2 T2S SD.SETT 020: MATCHING SERVICE ...................................................... 8

  4.3 T2S SD.SETT 030: ALLEGEMENT SERVICE ............................................... 10

    4.3.1 T2S DD.SETT 031: Settlement allegement service component ................. 10

    4.3.2 T2S SD.SETT 032: Cancellation allegement service component .............. 10

  4.4 T2S SD.SETT 040: SETTLEMENT SEQUENCING SERVICE ...................... 11

  4.5 T2S SD.SETT 050: SETTLEMENT POSTING SERVICE ................................... 12

    4.5.1 T2S SD.SETT 051: Settlement eligibility check service component .......... 12

    4.5.2 T2S SD.SETT 052: Provisioning service component .............................. 12

    4.5.3 T2S SD.SETT 053: Booking service component ....................................... 14

  4.6 T2S SD.SETT 060: OPTIMISATION SERVICE .............................................. 14
4.6.1 **T2S SD.SETT 061: Technical netting and optimisation algorithms service component** ............................................................... 15
4.6.2 **T2S SD.SETT 062: Prioritisation service component** ........................................................................................................ 15
4.6.3 **T2S SD.SETT 063: Partial settlement service component** .................................................................................................. 16
4.6.4 **T2S SD.SETT 064: Auto-collateralisation service component** ............................................................................................. 17
4.7 **T2S SD.SETT 070: REALIGNMENT SERVICE** ....................................................................................................................... 21
4.8 **T2S SD.SETT 080: INSTRUCTION RECYCLING SERVICE** ..................................................................................................... 21
4.9 **T2S SD.SETT 090: INSTRUCTION AMENDMENT SERVICE** .................................................................................................... 22
4.10 **T2S SD.SETT 100: INSTRUCTION CANCELLATION SERVICE** .............................................................................................. 23
4.11 **T2S SD.SETT 110: HOLD/RELEASE SERVICE** .................................................................................................................... 24
4.12 **T2S SD.SETT 120: EARMARKING, BLOCKING AND RESERVATION SERVICE** ......................................................................... 24
4.12.1 **T2S SD.SETT 121: Earmarking service component** ......................................................................................................... 24
4.12.2 **T2S SD.SETT 122: Blocking service component** ............................................................................................................ 25
4.12.3 **T2S SD.SETT 123: Reservation service component** ....................................................................................................... 25
4.12.4 **T2S SD.SETT 123: Common features of the earmarking, blocking and reservation service component** .......................................................... 26
4.13 **T2S SD.SETT 140: CONDITIONAL SECURITY DELIVERY (COSD) SERVICE** ................................................................. 27
4.14 **T2S SD.SETT 150: LINKED INSTRUCTIONS SERVICE** ......................................................................................................... 28
4.15 **T2S SD.SETT 160: CORPORATE ACTIONS SERVICE** ........................................................................................................... 29

5 **T2S SD.LIM: LIQUIDITY MANAGEMENT SERVICE CLASS** ........................................................................................................... 30
5.1 **T2S SD.LIM 010: LIQUIDITY TRANSFER SERVICE** ............................................................................................................. 30
5.2 **T2S SD.LIM 020: LIMIT MANAGEMENT SERVICE** .............................................................................................................. 33
5.3 **T2S SD.LIM 030: END OF DAY (EOD) CASH MANAGEMENT SERVICE** ..................................................................................... 34
5.4 **T2S SD.LIM 040: CORPORATE ACTION CASH SERVICE** ..................................................................................................... 35
5.5 **T2S SD.LIM 050: CASH BLOCKING AND RESERVATION SERVICE** ........................................................................................ 36
5.6 T2S SD.LIM 060: LIQUIDITY MONITORING SERVICE .................................................... 36
5.7 T2S SD.LIM 070: MULTIPLE LIQUIDITY PROVIDER SERVICE ................................. 38

6 T2S SD-STD: COMMON STATIC DATA MANAGEMENT SERVICE CLASS. 39
6.1 T2S SD.STD 010: COMMON STATIC DATA MANAGEMENT SERVICE ........................ 39

   6.1.1 T2S SD.STD 011: Insert service component ......................................................... 40
   6.1.2 T2S SD.STD 012: Update service component ....................................................... 40
   6.1.3 T2S SD.STD 013: Delete service component ......................................................... 40
   6.1.4 T2S SD.STD 014: Reactivate service component ................................................... 41
   6.1.5 T2S SD.STD 020: Securities Reference Data service ........................................... 41

6.2 T2S SD.STD 030: T2S PARTY DATA SERVICE ............................................................... 41
6.3 T2S SD.STD 040: SECURITY ACCOUNT DATA SERVICE ........................................... 43
6.4 T2S SD.STD 050: CASH ACCOUNT DATA SERVICE ................................................... 44
6.5 T2S SD.STD 060: T2S USER DATA SERVICE ................................................................. 45
6.6 T2S SD.STD 070: ROLES AND PRIVILEGES DATA SERVICE ...................................... 46
6.7 T2S SD.STD 080: RESTRICTION MANAGEMENT SERVICE ....................................... 47
6.8 T2S SD.STD 090: ATTRIBUTE DOMAIN DATA SERVICE (MARKET-SPECIFIC ATTRIBUTES) 49

7 T2S SD. INF: INFORMATION MANAGEMENT SERVICE CLASS .......................... 50
7.1 T2S SD.INF 010: STATUS MANAGEMENT SERVICES ................................................ 50
7.2 T2S SD.INF 020: REPORT GENERATION SERVICE ................................................... 50
7.3 T2S SD.INF 030: QUERY SERVICE ............................................................................ 52

   7.3.1 T2S SD.INF 031: Query service for T2S Actor service component .................... 53
   7.3.2 T2S SD.INF 032: Query service for CSDs service component ............................ 53
   7.3.3 T2S SD.INF 033: Query service for euro area or for non-euro area NCBs service component 53
7.3.4 T2S SD.INF 034: Query service for Payment Banks (liquidity providers) service component 54
7.3.5 T2S SD.INF 035: Settlement-related queries service component 54
7.3.6 T2S SD.INF 036: Cash balance-related queries service component 54
7.3.7 T2S SD.INF 037: Common Static Data-related queries service component 55
8 T2S SD. CON: CONNECTIVITY / COMMUNICATION SERVICE CLASS 57
8.1 T2S SD.CON 010: MESSAGING SERVICES 58
8.1.1 T2S SD.CON 011: Push messaging service component 58
8.1.2 T2S SD.CON 012: Pull messaging service component 59
8.1.3 T2S SD.CON 020: Technical validation services 59
8.2 T2S SD.CON 030: CONNECTIVITY TYPES SERVICES 60
8.2.1 T2S SD.CON 031: Application to Application (A2A) service component 60
8.2.2 T2S SD.CON 032: User to Application (U2A) service component 60
8.3 T2S SD.CON 040: INFORMATION SECURITY MANAGEMENT SERVICES 60
8.3.1 T2S SD.CON 041: Authentication service component 61
8.3.2 T2S SD.CON 042: Authorisation service component 61
8.3.3 T2S SD.CON 043: 4-eyes principle service component 62
8.4 T2S SD.CON 050: MESSAGE SEQUENCING SERVICES 62
8.5 T2S SD.CON 060: DIRECT CONNECTIVITY SERVICES 62
8.6 T2S SD.CON 070: ROUTING SERVICES 63
9 T2S SD. SUP: OPERATIONS AND SUPPORT SERVICE CLASS 64
9.1 T2S SD.SUP 010: T2S BUSINESS APPLICATION CONFIGURATION SERVICES 64
9.1.1 T2S SD.SUP 011: T2S Calendar service component 64
9.1.2 T2S SD.SUP 012: T2S Settlement Day service component 65
9.2 T2S SD.SUP 020: OPERATIONAL MONITORING SERVICES 66
9.3 T2S SD.SUP 030: BUSINESS CONTINUITY MANAGEMENT SERVICES 67
9.4 T2S SD.SUP 040: DISASTER RECOVERY AND CRISIS MANAGEMENT SERVICES 67
9.5 T2S SD.SUP 050: ARCHIVING SERVICES ................................................................. 68
9.6 T2S SD.SUP 060: T2S SERVICE DESK SERVICES .................................................. 68
9.7 T2S SD.SUP 070: SERVICE LEVEL MANAGEMENT SERVICES .............................. 69
9.8 T2S SD.SUP 080: INVOICING SERVICES ............................................................... 70
  9.8.1 T2S SD.SUP 081: T2S invoicing to CSDs and euro area or non-euro area NCBs service component 70
  9.8.2 T2S SD.SUP 082: CSDs / euro area or non-euro area NCBs invoicing support service component 71
9.9 T2S SD.SUP 090: CHANGE AND RELEASE MANAGEMENT SERVICES ............... 71
  9.9.1 T2S SD.SUP 091: Change Management service component .............................. 72
  9.9.2 T2S SD.SUP 092: Release Management service component ............................. 74
9.10 T2S SD.SUP 100: TEST AND TRAINING SERVICES ............................................ 75
  9.10.1 T2S SD.SUP 101: Testing service component ..................................................... 75
  9.10.2 T2S SD.SUP 102: Training service component .................................................... 75
1 T2S Service Description overview

1.1 Purpose of this note

This note provides a common base for the description of T2S Services, especially pertaining to the Framework Agreement and to the Currency Participation Agreement.

This T2S Service Description for the Operational Phase of T2S focuses on:

(1) providing a common structure for the services that T2S will deliver, i.e. settlement services, liquidity management, Common Static Data services, information services, Connectivity Services, operational and support services as well as the individual services;

(2) the content of the service from the T2S Users’ perspective, i.e. what services the T2S Users will receive, and the business perspective of the interchanges between T2S and the T2S Users; and

(3) the boundaries of the services T2S will deliver to its users, i.e. what is within the scope of T2S Services, and what is outside of the scope of T2S Services.

1.2 Scope of the T2S Service Description

1.2.1 Within the scope of the T2S Service Description

T2S is a technical solution to support Central Securities Depositories (CSDs) by providing core, borderless and neutral settlement services. The objective is to achieve harmonised and commoditised settlement in Central Bank Money (CeBM) in euro and other eligible currencies for substantially all securities in Europe.

The Eurosystem manages and operates the T2S Business Application and the technical solution providing the T2S Services, this service provision by the Eurosystem is hereafter referred to simply as “T2S”. The Contracting CSD will maintain full control over the business and contractual relationship with its customers.

The T2S Service Description describes all services T2S will deliver for the T2S Operational Phase including all services delivered to all Participating CSDs, to all Directly Connected Parties (DCPs), and to all participating euro area or non-euro area NCBs, once T2S is in full operation. The T2S Service Description itself is subject to the rules and procedures established for all Schedules and Annexes of the Framework Agreement.
1.3 Outside of the scope of the T2S Service Description

This Service Description describes only the services T2S will deliver during the Operational Phase. The services delivered by the T2S Programme during the Development Phase and the Migration Period are not described in this note.

The Service Description furthermore provides background and relevant information with regard to:

a. The Service Level Agreement (SLA\(^2\)), which will contain all Key Performance Indicators (KPIs), the latter will not be defined nor referenced in the Service Description.

b. The T2S technical architecture is not described in this Service Description and nor are the technical details required to establish the connectivity to T2S.

1.4 T2S Service Description and its relationship to other documents

The Service Description is a high level description of the Services T2S delivers during the Operational Phase thereby identifying the scope of the T2S Services and as such complementing the T2S Scope Defining Set of Documents.

Since, the Service Description is a high level description, in some parts of the Service Description it has been indicated in which documents, e.g. Business Process Description, User Handbook, Manual of Procedures (MoP), further and more detailed information can be found.

---

1 Details on the T2S Programme can be found in the Framework Agreement and its relevant Schedules
2 The SLA is a separate document linked closely to this Service Description. The Service Description describes the services T2S clients receive, the SLA defines the relevant KPIs, as well as their control and reporting procedures. Therefore, these two documentations are closely linked and harmonised
2 Service delivery framework

2.1 Scope of T2S instrument

In principle, T2S covers all securities that comply with the following eligibility criteria, i.e. that:

1. have an ISIN code, as instrument identifier;
2. can be settled via a CSD in T2S;
3. can be settled in book-entry form; and
4. are fungible (from a settlement process perspective).

Securities that do not fall within the scope of any connected CSD are not part of T2S either.

T2S can settle only securities that are compliant with the above criteria 1 to 3, certain securities, compliant with the first three criteria, but not compliant with criteria 4 (non-fungible from a settlement perspective), may still be entered in and processed by T2S.

T2S settles all eligible securities in a standardised settlement process.

2.2 Scope of T2S instruction and transaction type

The instruction types covered by T2S are the following:

- Settlement Instruction
- Liquidity Transfer
- Settlement Restriction
- Amendment Instruction
- Cancellation Instruction
- Hold / Release Instruction

T2S settles only settlement transactions with a CeBM cash leg (or no cash leg), it will not provide settlement in Commercial Bank Money (CoBM). T2S provides services for securities settlement and the related cash settlement using a number of transaction types:

- FOP (Free-of-Payment) consists of DFP (Deliver-Free-of-Payment) and RFP (Receive-Free-of-Payment). In both cases, securities are delivered / received without payment being made.
- DVP (Delivery-versus-Payment) and RVP (Receive-versus-Payment) define an exchange of securities for cash. DvP and RvP are both securities settlement mechanisms
which link a securities transfer and a funds transfer in such a way as to ensure that delivery occurs if - and only if - the corresponding payment occurs.

- DWP (Deliver-with-Payment) and RWP (Receive-with-Payment) is a type of instruction and settlement mechanism, specifying the delivery of securities together with a cash payment. For example, trade netting by a Central Counterparty (CCP), as an authorised CSD participant, may result in such instructions.

- PFOD (Payment-Free-of-Delivery) defines an exchange of cash without the delivery of securities.

3 T2S SD: Overview T2S Services

T2S deploys a flexible hierarchical party model to allow CSDs and euro area or non-euro area NCBs to manage their accounts and parties in an efficient way. Roles, including some of the key responsibilities, are allocated in line with the differentiation into:

- a securities’ perspective (CSDs); and
- a cash’s perspective (euro area and non-euro area NCBs).

The structure of this Service Description document is based on the above mentioned differentiation between the securities perspective (CSDs) and the liquidity management perspective (euro area and non-euro area NCBs)3:

- CSDs are the gateways through which various market parties can access T2S. Depending on their needs, a CSD’s participants may continue to contract with one or more CSDs for the settlement of their trades and collateral operations (and those of their customers) in T2S. Each CSD will set up and maintain its own Security Accounts’ structure in T2S. Each CSD is responsible for setting up and maintaining all CSD Static Data relating to the settlement activities of its participants. A T2S Actor settling through more than one CSD in T2S can have Security Account(s) with each of the CSDs it uses for settlement.

- All euro area and all non-euro area NCBs whose currencies are available for settlement in T2S have the responsibility to set up and to maintain Dedicated Cash Accounts

---

3 A more detailed description of the account structures deployed by T2S can be found in the User Detailed Functional Specifications (UDFS), chapter 1.2.6. Accounts structure and organisation
(DCAs) in T2S if they have concluded a relevant agreement with eligible entities. Furthermore, they are also responsible for setting up and maintaining all Central Bank Static Data relating to the DCAs of its members. Cash settlements in T2S take place exclusively on T2S DCAs. Only a CeBM account opened on the books of a euro area or a non-euro area NCBs whose currency is available for settlement in T2S may serve as a T2S DCA.

The totality of the T2S Services (level 1 of the service hierarchy description) are broken down into service classes (level 2 of the service hierarchy) and services (level 3). If the latter (level 3) contain functionally diverse components, level 4 of the service hierarchy describes these service components:

![Service Hierarchy Diagram]

(If required, Level 4 of the service decomposition will contain the service components)
4 T2S SD.SETT: Settlement services service class

4.1 T2S SD.SETT 010: Business validation service

Each instruction will go through the same T2S standard validations.

With the exception of the additional information fields as described below, the business validation service ensures that the content of the received message is valid, i.e. contains all required fields and complies with the rules defined for the content of these fields. These consistency checks ensure that the message can be processed by T2S as intended and is consistent with the relevant rules for this message stored in Common Static Data.

Business validation in T2S consists of two different types of validations:

1. Contextual checks, that is when the validation of one field is dependent on the content of another field, e.g. reference / Common Static Data or other data provided via the Graphical User Interface (GUI); and

2. Event-driven checks, e.g. settlement date change.
All incoming messages are validated when they enter T2S and re-validated (as are all pending instructions) at the start of a new Settlement Day. Updates of the Common Static Data used for business validation purposes result in revalidation of all relevant instructions. T2S assigns a status of matched/unmatched at the same time that the instruction is validated.

Messages sent by a T2S Actor to T2S may contain Additional Information Fields which T2S Actors may use for their own purposes. This additional information is neither required for nor related to any T2S process and is therefore neither validated nor further processed within T2S.

T2S stores this additional information together with the information it has processed.

Once T2S has successfully validated the compliance of the data - contained in the instruction with the data stored in Common Static Data relevant for the business validation process - the instruction is routed to the relevant processing module of T2S. If settlement-related process indicators are specified by the instructing T2S Actor, T2S checks that they are valid for the type of instruction and the instructing T2S Actor in question. The settlement-related process indicators are used to perform certain actions in the settlement process relating to an instruction. T2S Actors may use the non-settlement-related link indicator “INFO” to link instructions for information purposes.

In the event of instructions being held/released, cancelled, amended or that make use of a previous settlement restriction, T2S verifies that the previous or related reference exists. T2S performs the business validation on the maintenance/new instruction to ascertain that it is valid and consistent with the previous or related instruction. After identifying a validation error, T2S continues to validate as far as possible (taking into account potential interdependencies between the validated data). If validation errors are found, T2S reports all of them in a single message to the T2S Actor and rejects the instruction.

After successful validation, T2S stores the instruction, assigns the corresponding statuses and informs the instructing T2S Actor and its CSD of the validation result, depending on their message subscription preferences. Once validated:

- settlement instructions that require matching are forwarded for matching;
- maintenance instructions are forwarded to the maintenance functionality; and
- settlement restrictions are forwarded for settlement only on their Intended Settlement Date (ISD),

while all other instructions are forwarded directly to the settlement functionality.
T2S must support the CSDs and euro area and non-euro area NCBs by offering the capability to provide specific validations and processing of messages to fulfil Legal and Regulatory Requirements as well as supervisory requirements in the markets that they service. T2S therefore allows the CSDs and the euro area and non-euro area NCBs to define their own restriction types. T2S triggers a revalidation of all relevant recycled instructions when settlement-related Common Static Data change. T2S cancels instructions that do not pass the revalidation successfully and informs both the CSD and the instructing T2S Actor of the cancellation.

T2S validates all incoming and recycled instructions against rules and parameters defined in the Common Static Data for the configuration of restriction types. T2S thus checks and validates whether there are any applicable restrictions. If there are, and depending on the type of the restriction, T2S either accepts, rejects or puts the instruction on hold until it is released for further processing.

4.2 T2S SD.SETT 020: Matching service

The settlement instruction Matching service in T2S compares the settlement details provided by the buyer of securities with those provided by the seller of the securities in order to ensure that both parties agree on the settlement-related terms of an instruction.

T2S provides real-time matching, compliant with the rules of the European Securities Services Forum (ESSF)/European Central Depositories Association (ECSDA), throughout the operating day (except during the Maintenance Window). Matching in T2S is mandatory for cross-CSD settlements. Matching for intra-CSD settlements may take place in T2S or in the legacy systems of the CSD.

T2S only attempts to match validated settlement instructions that entered T2S as “unmatched”. If matching is successful, T2S assigns the match status “matched” to the settlement instructions and informs the T2S Actor of the matching of their settlement instruction. If T2S finds no corresponding unmatched counterpart instruction for the unmatched settlement instruction, the match status remains unchanged and T2S sends no information to the instructing T2S Actor.

T2S waits for the missing counterpart instruction for a predetermined period before generating an allegement message for the counterpart in the unmatched instruction. T2S sends the allegement message to the relevant counterparty only if the counterpart has subscribed to receive allegement messages.
T2S attempts to match the instruction for 20 working days (T2S calendar) after the Intended Settlement Date or the date of the last status change, in accordance with the ESSF/ECSDA recommendation. After 20 working days, T2S cancels the underlying instruction and informs the relevant T2S Parties.

T2S matches the settlement cash amount for T2S eligible settlement currencies with a certain tolerance level (i.e. in the event that there is no perfect match). The tolerance amount has two different bands per currency, depending on the counter value, in line with ECSDA rules. The general tolerance amount proposed by ECSDA for matching the settlement amount field in euro is currently €25 when the counter value is above €100,000 or €2 when it is €100,000 or less.

Once T2S has matched two instructions with a difference in the settlement amount that is less than the tolerance amount, T2S shall settle the instruction with the seller’s settlement amount.

T2S matches different types of fields:

1. Mandatory matching fields

   Mandatory matching fields are those fields that must exist in the instruction and which values should be the same in both Settlement Instructions except for (i) the Settlement Amount of DVP/PFOD instructions for which a tolerance might be applied; and (ii) the Credit/Debit Code (CRDT/DBIT); and (iii) the Securities Movement Type Deliver/Receiver (DELI/RECE), whose values match opposite (meaning that opposite values in instructions are considered as required to match the instructions).

2. Non-mandatory matching fields

   T2S supports two types of non-mandatory matching fields:

   a. Additional matching fields are fields that are initially not mandatory but become mandatory matching fields when either one of the counterparts to the settlement provides a value for them in its instruction. T2S cannot match a filled-in additional matching field with a field with no value (null / zero value).

   b. Optional matching fields are fields that are initially not mandatory:

      i. If only one T2S Party provides content in an optional matching field, T2S may match with a field with no value (null / zero value).

      ii. If both settlement counterparts provide a value for the same field in their instructions, then the optional matching field becomes mandatory for matching.
4.3 T2S SD.SETT 030: Allegement service

T2S uses allegement messages to inform counterparties that an instruction is missing. An allegement message advises an account owner that another T2S Actor has issued instructions against its account for which the account owner has no corresponding instruction in the Securities Settlement System. Allegements will be sent only if the counterparty has subscribed to receive such messages. T2S alleges a T2S Actor when a settlement instruction or a cancellation instruction is missing. Allegement messages may be used for any unmatched instruction that requires matching.

4.3.1 T2S DD.SETT 031: Settlement allegement service component

After the first unsuccessful matching attempt, T2S waits for the missing counterparty instruction for a predetermined period of time before generating an allegement message. If the instruction is still unmatched at the end of this period, an allegement message is generated. T2S sends an allegement message for the unmatched instruction only if the counterparty has subscribed to receive allegement messages.

T2S supports two standard delay periods for sending allegements to the counterparties of the unmatched instruction:

- “Allegement from first unsuccessful matching attempt”, as the standard delay period from the first unsuccessful attempt to match a settlement instruction.
- “Allegement before Intended Settlement Date”, as the standard delay period measured backwards from the FOP cut-off time on the intended Settlement Date.

T2S sends out the allegement at the earliest point in time between the two standard delay periods. T2S calculates the standard delay period in hours and minutes.

If the previous allegement message is no longer valid, T2S sends an allegement removal or an allegement cancellation. An allegement cancellation means the cancellation of an allegement message sent previously, due to a cancellation of the settlement instruction by the sender. An allegement removal acknowledges that an allegement message sent previously is no longer valid, because T2S has in the meantime received the missing instruction from the alleged T2S Party.

4.3.2 T2S SD.SETT 032: Cancellation allegement service component

T2S also provides allegement services in the event of a missing counterpart cancellation instruction, via a status advice message. T2S sends out the cancellation allegement without waiting for any predetermined period to have elapsed. The cancellation instruction remains pending until it matches with a valid counterpart cancellation instruction.
If the cancellation allegement sent via status advice is no longer valid because the revalidation of the settlement instruction has been unsuccessful, the counterparty has responded with a cancellation instruction, or the underlying matched settlement instructions have been settled, T2S sends only the settlement confirmation (in case of settled underlying instructions) and status advices (in case of cancelled underlying instructions) to both parties.

T2S does not send a status advice to the counterparty to communicate cancellation of the previous cancellation allegement.

4.4 T2S SD.SETT 040: Settlement sequencing service

Sequencing is the pre-determined order defined in T2S in which instructions are submitted for settlement.

During the Real-time Settlement, instructions are processed in the order in which they arrive for settlement.

For night-time settlement, sequencing refers to the order in which the settlement of certain sets of instructions is attempted in T2S. Settlement instructions are processed in a particular sequence, (i.e. in a fixed order) to avoid the use of security positions and/or cash resources for any transaction other than those submitted in the sequence concerned. T2S runs two settlement cycles with predefined settlement sequences during the night. In each settlement sequence, T2S will perform a settlement attempt for those settlement transactions selected based on the eligibility criteria of the sequence including:

- all new instructions with the current ISD entered into T2S until the launch of the current settlement sequence. These instructions include, for instance, settlement instructions providing liquidity via lending (securities lending) that are intended to settling instructions that could not be settled in an earlier settlement attempt; and
- all recycled instructions that could not be settled in an earlier settlement attempt. Such recycled instructions include all instructions that could not be settled in the previous settlement attempts.
4.5 T2S SD.SETT 050: Settlement posting service

The transactions are settled in T2S by booking the cash and securities debits and credits in accordance with the relevant instructions on the relevant T2S DCAs and Security Accounts (either accounts identified in the instructions being settled or accounts predetermined by default).

The settlement posting service consists of three service components:

- Settlement eligibility check
- Provisioning
- Booking

4.5.1 T2S SD.SETT 051: Settlement eligibility check service component

The settlement eligibility check is the final validation before settlement, as it is necessary to identify the appropriate instructions for the final settlement process. The eligibility check considers:

- the Intended Settlement Date (ISD);
- the potential blocking of the T2S Actor, Security Account, security or T2S DCA from settlement;
- whether or not the instruction is on hold; and
- whether the instruction is linked to other instructions,

before an instruction is submitted to the provisioning and booking process. T2S forwards for settlement only those instructions that meet the eligibility criteria for settlement. Settlement instructions which do not meet the eligibility criteria remain unsettled.

4.5.2 T2S SD.SETT 052: Provisioning service component

The provisioning or provision-check ensures that the eligible transaction can be forwarded for booking (and thereby finally settled) if, and only if, the booking does not cause the account balances of the relevant securities and the T2S DCA to become negative, with the exception of T2S euro area and of T2S non-euro area NCBs own accounts, T2S transit accounts and Issuer CSD balance accounts, which may have negative balances.

The provision-check covers both settlement legs of the relevant transaction (e.g. the cash and securities legs for a DvP transaction). T2S does not consider reserved/blocked securities quantities or cash amounts on the relevant accounts as available for the provision-check, unless the instruction being settled refers to the initial reservation/blocking instruction.

When an individual external guarantee limit, unsecured credit limit or auto-collateralisation limit
is defined by the relevant euro area and non-euro area NCBs (or by the relevant Payment Bank for the settlement of the instructions of the T2S parties for which it provides cash settlement services), T2S ensures that the net cash debit resulting from the booking of any instruction(s) of the relevant T2S parties does not exceed the unused part of this external guarantee limit, unsecured credit limit or auto-collateralisation limit.

T2S performs the provision check in the following sequence:

1. Provision check of available securities position on the Security Account (only for the settlement of securities).
2. Provision check for the T2S DCA and auto-collateralisation (if required).
3. Provision check on the external guarantee limit.
4. If auto-collateralised: provision check on the auto-collateralisation limit of the client of the Payment Bank.
5. Provision check on the unsecured credit limit.

When several instructions are submitted together in a settlement attempt, the provision-check considers the final net balance resulting from the booking of all the relevant instructions (and not from each and every instruction). In other words, in its provision-check T2S takes into account the technical netting effect.

If the provision-check on the net balance is not satisfactory, T2S identifies the instruction(s) responsible for the provision-check’s failure.

These instructions are either:

- submitted for an auto-collateralisation process if the fail originates from a lack of cash;
  - or,
- submitted for partial settlement (only as a last resort, i.e. if auto-collateralisation is not possible or not sufficient and only if the instructions are eligible and are within the partial settlement window) if the fail originates from a lack of securities or from a required substitution of collateral.
4.5.3 T2S SD.SETT 053: Booking service component

Final booking is only posted if the provision-check on the accounts (securities and T2S DCAs) referred to in the settlement instructions (or on the accounts predetermined by default) is satisfactory.

Once booked by T2S on the T2S parties’ Security Accounts and T2S DCAs, cash and securities debits and credits are final, i.e. irrevocable and unconditional. The booking must not be conditional on any external event (e.g. such as another booking in the payment or settlement system/arrangement of an external euro area or non-euro area NCBs registrar, commercial bank or CSD), this means that any such condition must have been resolved before the booking in T2S is undertaken.

Because bookings are final, T2S will not automatically unwind credit or debit even if it was done incorrectly.

Each and every transaction is booked on a gross basis. This is without prejudice to the use of the technical netting effects in the provision check when several instructions are submitted together for settlement (either for optimisation purposes or because they are linked by a T2S Actor).

4.6 T2S SD.SETT 060: Optimisation service

T2S optimisation services is intended to determine the optimum balance between maximising the volume and the value of the settlement with the available securities, in order to minimise the number and value of unsettled instructions at the end of the night-time settlement process as well as to minimise the number and value of fails at the end of the Settlement Day.

Optimisation procedures are specific processes aimed at increasing settlement efficiency. Such processes detect and resolve settlement gridlocks, and perform technical netting of obligations in cash and securities, with a view to settle new instructions as well as instructions that could not be settled when previously attempted. Optimisation procedures are available both during the night-time settlement window and during the Real-time Settlement. When several unsettled instructions are optimised together and a chain of instructions is submitted for settlement, T2S includes the securities and cash received during the process of settling the relevant chain of instructions in the optimisation process.

During the night-time settlement window, the T2S optimisation procedure covers all instructions submitted for settlement (either new instructions or recycled instructions that could not be settled when previously attempted).

During the Real-time Settlement, T2S optimisation procedure runs in parallel to real-time
settlement processes and covers instructions that could not be settled when previously attempted. When necessary, T2S combines the four optimisation procedures described below (technical netting/optimisation algorithms, prioritisation, partial settlement and auto-collateralisation).

4.6.1 T2S SD.SETT 061: Technical netting and optimisation algorithms service component

The technical netting is intended to limit the resources necessary for the settlement of a set of instructions submitted together for settlement. Without prejudice to the fact that booking takes place on a gross basis, T2S reduces, through technical netting, the final net balance to be credited and debited on Security Accounts and/or Dedicated Cash Accounts. When performing its provision-check, T2S considers the final net balance that results from the booking of all the instructions submitted together for settlement (and not that resulting from each and every individual instruction).

During the night-time settlement window, T2S submits all eligible instructions for settlement and optimises all these instructions together. During day-time, real-time settlement optimisation, optimisation algorithms identifying chains of instructions (e.g. such as empty circles, back-to-back instructions) are used to resolve gridlock situations, and to increase the volume and value of settlement and hence, to reduce the value and volume of pending instructions.

4.6.2 T2S SD.SETT 062: Prioritisation service component

Optimisation procedures will take into account the four different priority levels of instructions. T2S automatically assigns predetermined levels of priority for certain specific instructions identified in the Common Static Data. The four different levels of priority identified are:

1. Reserved priority: Only Participating CSDs and euro area or non-euro area NCBs can assign a “reserved priority” for specific instructions such as intraday corporate actions or certain euro area and non-euro area NCBs’ specific operations related to the provision/reimbursement of their credit operations.

2. Top priority: T2S automatically assigns top priority to transactions of trading platforms (MTFs, stock exchanges, etc.) with and without CCP and OTC instructions with CCP. To that end, the parameters for identifying transactions (to which this top priority level must be assigned) are predetermined in Common Static Data and apply by default to all the relevant transactions. T2S does not allow top priority to be assigned to any other category of transactions (either by default or at a transaction level).

3. High priority: T2S Actors can assign high priority to their settlement instructions; or

4. Normal priority: T2S assigns normal priority to all other instructions, but enables T2S parties to assign them a high priority on an instruction-by-instruction basis.

For levels 3 and 4 only, the instructing T2S Actor may change the priority level of an instruction
(only the deliverer may change normal priority to high priority or high priority to normal priority).

T2S optimises and recycles settlement instructions in accordance with their priority levels in such a way that if several instructions compete for use of the same securities and/or cash resources, for settlement purposes preference is given to the instruction with the highest level of priority. In addition to the priority level, T2S also considers the ISD of the instruction so as to favour the settlement of instructions with the earliest settlement date and thus avoid instructions with low priority not being settled.

For Real-time Settlement, the prioritisation applies only to instructions to be recycled in the settlement queue (i.e. failed instructions). Any increase of a position triggers an optimisation for the International Securities Identification Number (ISIN) concerned. T2S recycles instructions if there is insufficient position.

Furthermore, during the Real-time Settlement, the priority level is taken into account by the settlement procedure only for instructions that failed to settle in a previous settlement attempt. These are subsequently submitted for recycling and optimisation procedures.

4.6.3 T2S SD.SETT 063: Partial settlement service component

T2S uses partial settlement for instructions that could not be settled due to the lack of securities providing the settlement instruction fulfils all criteria for partial settlement. A lack of cash does not trigger partial settlement. Instructions linked by T2S Actors are excluded from partial settlement (see UDFS for further details).

The partial settlement procedure is used for all T2S instructions, unless one of the counterparts indicates at instruction level that partial settlement is not allowed (partial indicator set to no/false), and if the following conditions are met:

- the partial settlement threshold criteria are met, set for both securities and cash, and defined as part of the Common Static Data; and
- the partial settlement window is active.

When submitting an unsettled instruction for partial settlement, T2S attempts to settle the maximum quantity of securities available on the Security Account of the seller, taking into account the threshold chosen by the counterparts.

Once partial settlement has been invoked, T2S allows a duly authorised Actor to modify only the priority of the instruction, or to hold, to release or to cancel the pending part of a partially settled instruction. When an instruction is partially settled, T2S does not automatically cancel the original instruction. T2S keeps the original instruction and updates in accordance with the partial
settled volumes in the status management.

Reverse collateral instructions are not subject to partial settlement.

T2S uses its own partial settlement parameter to activate and de-activate partial settlement as part of the continuous optimisation process. T2S allows the definition of several T2S parameters for activating and deactivating the partial settlement procedure during the night-time and day-time settlement periods. The T2S partial settlement parameter defines at which moment in time or based on which event T2S activates or de-activates a partial settlement procedure.

In order to minimise fails due to a lack of securities, T2S allows partial settlement in specific time windows, a predefined period before the end of Real-time Settlement and at the end of the last night time cycle during the night-time settlement. T2S submits to partial settlement all eligible instructions that failed to be settled in a previous attempt during the night and deactivates the partial settlement functionality at the closure of the night-time settlement period (see UDFS).

T2S submits at least once all those instructions for partial settlement that it has identified as eligible for partial settlement before the partial settlement procedure is deactivated.

T2S informs the CSD and/or the DCP when partial settlement occurs, depending on the message subscription preferences.

4.6.4 T2S SD.SETT 064: Auto-collateralisation service component

T2S provides auto-collateralisation functionality during the whole T2S settlement period in order to facilitate the settlement of underlying securities-related instructions that would fail to settle due to a lack of cash on a Dedicated Cash Account (DCA) and/or insufficient external guarantee headroom on a Credit Memorandum Balance (CMB)⁴. T2S provides the auto-collateralisation service on the basis of the list of eligible collateral, relevant prices and limits provided by the euro area or by the non-euro area NCBs and Payment Banks.

The auto-collateralisation functionality with euro area and non-euro area NCBs and with Payment Banks is available to eligible T2S parties as defined in Common Static Data, provided that auto-collateralisation headroom is available. T2S triggers auto-collateralisation with euro area and non-euro area NCBs in case of lack of cash on the T2S DCA of the Payment Bank to which the settlement instruction is referring. T2S triggers auto-collateralisation with a Payment Bank (client-collateralisation) in the event of insufficient external guarantee headroom on the CMB of a client of the Payment Bank, that owns the Security Account to which the settlement instruction is referring.

---

⁴ Further described in the relevant chapter of the Liquidity Management Services below.
instruction refers.

T2S allows collateral provided for intraday credit provision in CeBM through auto-
collateralisation to be pledged or transferred to a separate account (in accordance with the legal
framework chosen by the relevant euro area or non-euro area NCBs). Collateral provided for
auto-collateralisation with Payment Banks can only be transferred to a separate account of the
Payment Bank. Intraday credit granted in CeBM through auto-collateralisation can be used only
for the settlement of the underlying instructions. The credit amount provided is equal or less than
the collateral value of the securities used as collateral, the collateral value being the price
provided for a certain security multiplied by the number or nominal amount of the security
concerned.

An intraday credit provision through auto-collateralisation is always fully collateralised in T2S

- Either with securities already held by the buyer via collateral-on-stock, or
- Through collateral-on-flow via the eligible securities that are being purchased.

These securities must be recognised as eligible collateral by euro area or non-euro area NCBs or
Payment Banks and the relevant Payment Bank or its clients must earmark them for their use as
collateral. Duly authorised T2S Actor may also earmark a Security Account from which
securities may be used for auto-collateralisation. The security account holding the earmarked
securities must be linked to the DCA opened by the euro area or by the non-euro area NCB.

In order to provide intraday credit through auto-collateralisation in T2S to one or several eligible
Payment Banks, each euro area and each non-euro area NCB has to open a T2S euro area or non-
euro area NCB cash account on which all debits corresponding to its intraday credit provisions
through auto-collateralisation will be posted. The T2S euro area or non-euro area NCB cash
account is allowed to have a negative cash balance.

The Payment Banks must open one Security Account (via their CSD) dedicated to auto-
collateralisation for each of their clients. T2S uses these accounts when transferring the collateral
from the client to the Payment Bank. If allowed by the respective euro area or non-euro area
NCB, the Payment Banks may use the securities positions received during the client-
collateralisation procedure as collateral for auto-collateralisation procedure with the euro area or
non-euro area NCBs. In such cases, the Payment Bank has the option to either earmark the
Security Accounts for auto-collateralisation purpose only or earmark specific securities positions
in the Security Account for auto-collateralisation. The Payment Bank will be able to use such
Security Accounts for both (a) receiving collateral in case of client-collateralisation (b) and
providing collateral for auto-collateralisation with euro area and non-euro area NCBs.
Each euro area and each non-euro area NCB is required to determine in Common Static Data the collateralisation procedure for which it opts, i.e. (i) transfer to an account opened in the euro area or non-euro area NCB’s name, or (ii) transfer to an account pledged in its favour, or (iii) reservation of securities. This must be done for all eligible Payment Banks to which the relevant euro area or non-euro area NCB provides intraday credit through auto-collateralisation.

For each of their Security Accounts, T2S parties may indicate via the T2S earmarking service whether T2S may use securities from that account when generating auto-collateralisation operations with euro area or non-euro area NCBs or Payment Banks on a specific T2S DCA. When such a link exists between a Security Account and a T2S DCA, T2S will use securities from that account in auto-collateralisation operations with either euro area or non-euro area NCB, or with the Payment Bank (acting as credit provider), depending on the earmarking options.

T2S generates auto-collateralisation operations only when they allow the settlement of the underlying settlement transaction(s) and when sufficient headroom exists on the auto-collateralisation limit. When triggering auto-collateralisation, T2S also considers the unsecured credit limit headroom available that could complement the auto-collateralisation operation in the event of auto-collateralisation with Payment Banks (client-collateralisation). Each euro area or non-euro area NCB and each Payment Bank is able to increase or decrease at any moment of the Settlement Day the auto-collateralisation limit of an eligible Payment Bank or client of the Payment Bank.

T2S submits auto-collateralisation instructions for settlement on an all-or-none basis together with the underlying settlement instructions in order to ensure that the amount of intraday credit provided through auto-collateralisation is automatically and exclusively used to settle the underlying instruction(s).

On the basis of the type of collateral movement chosen by each euro area or non-euro area NCB providing credit, T2S will collateralise the intraday credit provided through auto-collateralisation either:
by transferring the securities from the Security Account of a T2S Actor to the Security Account of the euro area or non-euro area NCB providing the credit;

- by transferring the securities from the account of the bank receiving the credit to another account of this Payment Bank (the second Security Account being pledged to the euro area or non-euro area NCB providing the credit where the securities are in the name of the bank receiving the credit); or

- by blocking the securities on the Security Account of the Payment Bank receiving the credit; in such a case, the securities will be blocked in favour of the euro area or non-euro area NCB providing the credit and T2S will not allow the Security Account holder to use the relevant securities as long as they are blocked.

When auto-collateralisation on flow and on stock are both possible for the settlement of a transaction or a set of transactions, T2S prefers to resorts to auto-collateralisation on flow before auto-collateralisation on stock. When the collateral value of the securities on flow is not sufficient to cover the amount of credit granted, T2S complements collateral on flow with collateral on stock. Finally, when securities being purchased in the underlying transaction are not eligible collateral (e.g. equities for Eurosystem intraday credit) and therefore cannot be used as collateral on flow, T2S uses collateral on stock to secure the amount of intraday credit granted through auto-collateralisation.

Whenever T2S generates and settles an auto-collateralisation operation, it creates and sets on hold the reimbursement of that auto-collateralisation operation - and the exact reverse operation (i.e. same amounts, same accounts, etc). The Payment Banks are able to trigger the reimbursement of their auto-collateralisation operations with euro area or non-euro area NCBs and with their clients at any moment during the daytime real-time settlement by releasing the relevant on hold reimbursement instructions.

Auto-collateralisation provides intraday credit that must be repaid at the end of the day. T2S uses all available liquidity on the cash accounts of the Payment Bank to repay the credit. In normal situations, the Payment Banks have repaid all intraday credit operations with the euro area or non-euro area NCBs before the auto-collateralisation reimbursement is initiated. If this is the case, T2S executes only a cash sweep during which the excess liquidity on the payment bank’s cash accounts is transferred to the relevant Real-Time Gross Settlement (RTGS) systems. If, however, there is not sufficient liquidity on the cash account at the end of the day to fully reimburse the pending intraday credit, special end of day procedures are invoked.

The securities that are held on the accounts of the euro area or non-euro area NCB (or pledged) for auto-collateralisation purposes are transferred to the overnight collateral Security Account.
indicated by the euro area or non-euro area NCB. At the same time, the relevant collateral
management system is informed of the move and the credit usage limit for the participant in the
RTGS system is increased. This process ensures that the T2S service provides, though a
collateralised credit, the same amount of liquidity in the RTGS system as it withdraws5.

4.7 T2S SD.SETT 070: Realignment service

When T2S matches a pair of settlement instructions, or receives an already matched pair of
instructions, it verifies whether the instructions submitted require realignment instructions on
accounts other than those of the T2S Parties submitting the instructions (e.g. on the accounts of
the Issuer CSD). If T2S identifies a need to realign, it generates the required realignment
instructions, on the basis of the cross-CSD links in the Common Static Data, automatically
validates the realignment instruction, and links all settlement instructions to ensure all-or-none
settlement.

If the Issuer CSD is within T2S and the Investor CSDs are not in T2S, the realignment takes
place in T2S on the basis of settlement instructions (usually free-of-payment) to be sent by the
Issuer CSD.

T2S does not send realignment instructions to the Issuer CSD if the Issuer CSD is outside T2S:

- The realignment process is handled by the Investor CSDs in coordination with the Issuer
  CSD outside T2S.

- If at least one Investor CSD is within T2S, the Conditional Securities Delivery (CoSD)
  mechanism can be used by the Investor CSDs, to block the position in T2S and hold the
  instruction until the settlement is confirmed in the Issuer CSD's books.

4.8 T2S SD.SETT 080: Instruction recycling service

Recycling occurs in anticipation of finding the required securities and/or cash subsequent
settlement runs, so that failed transactions can be settled successfully.

Recycling differs slightly depending on whether it occurs during day-time and night-time
settlement. In case of night-time settlement, all unsettled settlement instructions are recycled
automatically to the next settlement sequence. In day-time settlement, unsettled settlement

5 Further details especially on the reimbursement procedures and rules can be found in the User detailed Functional
Specifications, especially chapter 1.1.2 Liquidity management, and in the General Functional Specifications (GFS),
especially chapter 2.3.5 Liquidity Management
instructions are recycled when new settlement resources (i.e. securities and/or cash) become available.

Unmatched pending instructions are recycled for 20 days before cancellation by T2S. Matched pending instructions which fail to settle are recycled indefinitely.

The T2S settlement optimisation techniques reduce the number of unsettled settlement instructions at the end of the settlement day (EOD).

4.9 T2S SD.SETT 090: Instruction amendment service

T2S Actors may amend only process indicators, irrespective of the status of the underlying settlement instruction (except for instructions with an end-of-life status). The instructing T2S Party has to cancel and reinstruct the settlement if it wishes to modify any other fields.

T2S allows the amendment of the following process indicators until settlement occurs:

- partial settlement (only for settlement instructions);
- linking instructions; and
- settlement priority.

In case of partially settled instructions, the instructing T2S Party may amend the settlement priority only for the pending part of partially settled instructions.

T2S does not allow any settled or cancelled settlement instruction to be modified.

T2S will reject an amendment sent by a CSD participant other than the T2S Party which submitted the original instruction concerned, or its CSD, if the instruction to be amended was sent as non-modifiable by the CSD or an authorised CSD participant.

T2S informs the instructing T2S Party, as well as any T2S Actor duly authorised to access this information, immediately after the successful amendment of an instruction, in accordance with their message subscription preferences.

If the amendment process fails in T2S, then the amendment instruction is rejected. (e.g. original instruction has settled.)
4.10 T2S SD.SETT 100: Instruction cancellation service

Any instructing T2S Actor or its CSD may cancel its settlement instructions unilaterally prior to matching or its settlement restrictions prior to settlement. In such case, T2S verifies that (a) the instruction that the T2S Actor wishes to cancel exists in T2S and that (b) its cancellation is possible. Whether or not T2S Actors are able to cancel their instructions depends on the status of the instruction.

T2S will reject any cancellation request sent by a CSD participant other than the T2S Party which submitted the original instruction concerned, or its CSD, if the instruction to be cancelled has been sent as non-modifiable by the CSD or an authorised CSD participant.

Under the same rules, a CSD may cancel any instruction of any of “its DCP”. Cancellation instructions cannot be cancelled.

Until matching has occurred, T2S allows a T2S Actor to request unilaterally the cancellation of settlement instructions only.

Once matching has occurred, T2S Actors may cancel matched settlement instructions only bilaterally, i.e. both parties must send a cancellation instruction (“binding matching”) for the cancellation to take effect. T2S then matches the cancellation instructions and cancels both settlement instructions.

In the case of bilateral cancellation of settlement instructions, T2S checks whether the cancellation instruction from the counterpart exists and matches the two cancellation instructions. If the counterpart cancellation instruction does not exist, then the cancellation instruction remains pending until it matches with a valid counterpart cancellation instruction. T2S also accepts already matched cancellation instructions to cancel an instruction previously sent as already matched.

In the case of a Conditional Settlement (CoSD), T2S allows only the administering T2S Party identified in the Common Static Data to unilaterally request the cancellation of the instruction that triggered the CoSD process (e.g. when the external condition for settlement is not fulfilled), even after T2S has blocked the relevant securities holding for a CoSD. If a CoSD involves more than one administering T2S Party, the CoSD settlement instruction cannot be cancelled unless T2S receives cancellation instructions from each administering T2S Party involved in the initial settlement instruction.

T2S notifies the originator of a cancellation instruction when the cancellation instruction has either been executed (i.e. cancellation of the settlement instruction was successful) or denied (i.e. settlement instruction could not be cancelled). In the latter case, the resulting cancellation status
value for the cancellation instruction is “denied”.

If the cancellation process in T2S fails, then the cancellation instruction goes through recycling until it is either processed or rejected if the original instruction has already settled.

If the cancellation mechanism is automatically activated by T2S for a given instruction, T2S informs the CSD or the DCP that the instruction was cancelled by T2S. Automatic cancellation rules are applied to invalid or unmatched or failed/outdated instructions, and are compliant with ECSDA recommendations.

Realignment instructions cannot be cancelled by any T2S Actor.

4.11 T2S SD.SETT 110: Hold/release service

Hold and release mechanisms allow T2S Actors to hold or release settlement instructions until their actual settlement or cancellation, even beyond their Intended Settlement Date (ISD). These mechanisms give T2S Actors the flexibility to delay the settlement. T2S Actors may send maintenance instructions to hold and release settlement instructions as many times as required.

T2S allows only the T2S Actor that has put an instruction on hold to release it. If there are two executed hold instructions for the same instruction (i.e. one from the CSD participant and one from the CSD), release instructions must also come from both. If T2S receives a hold instruction for a settlement instruction that is already on hold or has been cancelled from the same T2S Actor who has submitted the initial hold or cancellation instruction, T2S denies the hold instruction.

T2S will reject any hold/release instruction sent by a CSD participant other than the T2S Party which submitted the original instruction, or its CSD, if the instruction to be held/released was sent as non-modifiable by the CSD or an authorised CSD participant.

All instructions on hold at the end of the ISD remain unsettled and T2S recycles them in accordance with the T2S rules for recycling instructions. Furthermore, T2S allows the remaining part of partially settled instructions to be held and to be released.

T2S will reject any hold or release settlement instruction if T2S has already settled or cancelled the underlying settlement instruction. T2S informs the instructing T2S Party accordingly, depending on its message subscription preferences.

4.12 T2S SD.SETT 120: Earmarking, blocking and reservation service

4.12.1 T2S SD.SETT 121: Earmarking service component

In T2S Parties may define that a security position or a security account be earmarked as a settlement restriction. For a position or an account to be earmarked, the securities must be fully
Earmarking defines that a security position or security account may be used for one and only one defined purpose. An earmarked position or account cannot be used for another purpose unless the earmarking is revoked.

A T2S Actor may earmark a position or an account for a specific purpose such as auto-collateralisation. If there is a conflict regarding use of the earmarked securities for a delivery/receipt owing to contradictory choices between account level and instruction level (that is to say when a settlement instruction refers to a earmarking purpose which is different from that at account level), the choice at account level overrides the choice at position level (T2S will credit or debit the earmarked position according to the purpose at account level and not according to the purpose at the instruction level). If earmarking is done at the Security Account level for a specific purpose, it will not be possible to earmark securities at position level (in the same account), for a different purpose.

Earmarking is not possible for DCAs.

4.12.2 T2S SD.SETT 122: Blocking service component

In addition to earmarking, T2S Parties may block securities or cash using settlement restrictions. Also via a static data maintenance it is possible to block securities account, DCA and Party in order to prevent settlement. A T2S Actor may block securities or cash for a specific purpose. For the securities or cash to be unblocked, the relevant instruction must contain the reference to the specific purpose.

A blocking of cash or securities prevents the transfer of specific securities/cash from a specific Security Account/T2S DCA.

When a blocking restriction is submitted for settlement, and providing sufficient securities and/or cash are available on the relevant accounts, T2S blocks the number of securities and/or the amount of cash specified in the settlement restriction on the relevant securities and/or T2S DCA(s). If insufficient securities and/or cash are available, the blocking will be recycled until full settlement can occur.

4.12.3 T2S SD.SETT 123: Reservation service component

As a further settlement restriction, T2S Parties may reserve securities or cash. A T2S Actor may create a reservation without having all the securities or cash specified in the reservation. Any securities or cash arriving will be attributed to the reservation until the reserved volume has been reached.

When a reservation instruction is submitted for settlement, and providing sufficient securities
and/or cash are available on the relevant account(s), T2S reserves the number of securities and/or
the amount of cash specified in the settlement instruction on the relevant securities and/or T2S
DCA(s). If insufficient securities and/or cash are available, T2S:

- reserves the securities and/or the cash already available on the relevant account; and
- supplements it with any incoming securities and/or cash proceeds arriving on this account, provided that the latter are not defined to be used for any other purpose.

A reservation of cash or securities reserves a securities or cash position for the settlement of one or more settlement instructions. A T2S Actor may refer to an existing reservation in another settlement instruction, by means of the reservation’s unique reference number. If such references result is made the provisioning process will include the reserved cash or securities in its provisioning check. The reserved securities/cash will be used first (ahead of unreserved securities/cash) for settlement of the instruction.

4.12.4 T2S SD.SETT 123: Common features of the earmarking, blocking and reservation service component

When several reservations/blockings of securities and/or cash have been performed on the same Security Account and/or T2S DCA, and a T2S Actor submits to T2S a settlement instruction referring to one (or some) of those reservation/blocking instructions, the T2S provision-check does not consider the additional securities and/or cash reserved/blocked through reservation instructions other than those referred to in the instruction being settled. However, if the securities/cash reserved/ blocked are not sufficient, T2S also takes into account additional securities and/or cash available on the relevant Security Account and T2S DCAs, provided that the latter have not been reserved/blocked for any other purpose.

If at EOD the reserved and blocked cash has not been used for any purpose, T2S releases the relevant cash. In case of a CoSD blocking, T2S releases the blocked cash at the EOD and creates a new CoSD blocking instruction. As regards securities, if blocked or reserved securities have not been used or released at EOD as a result of an instruction from the relevant T2S Actor, T2S does not release them automatically.
4.13 T2S SD.SETT 140: Conditional Security Delivery (CoSD) service

Conditional Security Delivery (CoSD) is a special functionality which manages instructions that require the fulfilment of a settlement condition outside T2S before securities may be settled in T2S. It is the responsibility of the CSD to set up, maintain and administrate the CoSD rule-based model and process. These rules are stored as part of the Common Static Data in T2S. Each rule identifies an administering T2S Party to release the instruction for settlement or to cancel the CoSD flagged settlement instruction and determines events which will result in an instruction automatically being submitted to the CoSD functionality by T2S. One settlement instruction might be subject to more than one CoSD rule and in such cases more than one administering T2S Party is assigned to that instruction.

On the ISD, T2S verifies all instructions with that particular ISD in accordance with the CoSD rules. It submits them automatically to the CoSD procedure if one or more CoSD rules are met. In such case, T2S automatically generates a settlement restriction to block the securities position, the cash position, or both. T2S rejects any cancellation request coming from the instructing parties after the activation of the CoSD process, as only administering parties are allowed to cancel settlement instructions submitted to CoSD.

T2S blocks the securities in the deliverer’s Security Account irrespective of the instruction to which the CoSD rule applies (similar rule applies for cash blocking on the T2S DCA linked to the receiver's Security Account). If two or more CoSD rules apply to the securities delivery instruction or related receiving or realignment instructions and those rules require securities to be blocked, the securities are blocked only once. Likewise, T2S blocks cash only once in the delivering cash account.

In a CoSD, securities, cash or both remain blocked and the instruction concerned remains on hold until T2S receives from the administering parties:

- a release instruction, requesting settlement of the instruction using the previously blocked securities or cash (on the basis of the information contained in the initial instruction); or

Further details can be found in the User Detailed Functional Specifications (UDFS), especially chapters 1.1.1. Settlement, 2.4 Send Settlement Restriction on Securities Position, 2.6 Send Release Instruction for CoSD by Administering Party, and 2.7 Send Cancellation Instruction for CoSD by Administering Party.
a cancellation instruction. After receiving cancellation instruction(s) from all administering parties T2S will cancel the CoSD instruction and its underlying instructions. In such case the underlying cash/securities are unblocked and the administering parties and instructing parties receive a confirmation message.

A “blocking” status message is sent by T2S to inform the (administering) CSD and/or the DCP that the securities, cash or both have been blocked for the processing of the original instruction. A “hold” status message is sent by T2S to inform the (administering) CSD and/or the DCP that the instruction related to the original instruction is prepared for settlement and waiting for release. Only the administering T2S Party can send the release message. If the receiving party is outside T2S, the status information is relayed by the CSD responsible for the account within T2S.

If the CoSD blocking cannot take place, T2S recycles the blocking instruction for the following Settlement Day. Cash blocked under CoSD is released at the EOD and regenerated for the following Settlement Day. Settlement instruction that are on CoSD Hold are recycled for the following Settlement Day (i.e. securities remain blocked and the settlement instruction remains on hold).

If the realignment chain changes or revalidation of the instruction submitted to CoSD and its related instructions is unsuccessful, T2S cancels all the instructions but the blocked securities/cash remain blocked.

**4.14 T2S SD.SETT 150: Linked instructions service**

T2S Actors may link instructions in order to ensure that a settlement instruction settles at the same time, before or after another settlement instruction. Linked instructions are possible on a one-to-one; one-to-many; or many-to-many basis.

When T2S submits several linked instructions for a settlement attempt, it posts the debits and credits for cash and securities from the relevant transactions if the provision check (including account netting effects) is successful. T2S settles sets of linked instructions according to the highest level of priority accorded to any of the instructions within the set (the whole set of linked instructions settles according to this level of priority).

T2S Actors can link instructions by using the ISO settlement link indicators “AFTER”,
“BEFORE” and “WITH”. These link indicators will be used in the settlement process. It is also possible to link by using a pool reference, which behaves from a settlement point of view as a WITH link. In addition, the T2S actors can use the INFO link, which has no impact on the settlement processing.

When T2S receives an instruction which is linked to one or more other instruction(s), it:

1. Checks that the linked instruction(s) exist.
2. Then validates that the information contained in the new linked instruction is consistent with the instruction which exists and to which it is linked, i.e. the ISD and the Security Account holder used are the same.

Linked instructions are excluded from partial settlement. If at EOD a linked instruction has not been settled it will be recycled.

4.15 T2S SD.SETT 160: Corporate actions service

To support the CSDs in settling corporate action entitlements, T2S uses standard settlement services for security settlement as well as liquidity management/cash settlement.
5 T2S SD.LIM: Liquidity Management Service Class

5.1 T2S SD.LIM 010: Liquidity transfer service

A liquidity transfer in T2S is an instruction from a DCA holder to transfer a specified amount of cash balance from its cash account to another cash account. The T2S DCA holders are Payment Banks or euro area or non-euro area NCBs.

T2S allows a T2S DCA holder to receive liquidity on its T2S DCA(s) from any RTGS account (provided that they are denominated in the same currency and that this is permitted by the relevant euro area or non-euro area NCB). In the same way, T2S allows the holder of the T2S DCA to send liquidity from its T2S DCA(s) to any RTGS account (as setup by the relevant euro area or non-euro area NCB in T2S) if the currency is the same.

In addition to liquidity transfers between RTGS accounts and T2S as mentioned above, T2S provides T2S DCA holders with a “multiple liquidity providers” functionality, i.e. T2S DCA holders can receive liquidity from and reimburse to several RTGS accounts.

Liquidity transfers are executed in real time upon receipt. During the execution of the liquidity transfer, if the status of the liquidity transfer order changes, T2S informs the T2S Actor about the new status if the latter’s message subscription rules in the Common Static Data so dictate.
T2S supports three types of liquidity transfers between T2S DCAs and RTGS cash accounts and between T2S DCAs.

- **Immediate liquidity transfer order:**
  
  - Liquidity is transferred in real time on receipt of the instruction from the account holder or a T2S Party with the appropriate rights.
  
  - Used to transfer liquidity between a T2S DCA and the RTGS account or between two T2S DCAs (if these DCA belong to the same Payment Bank or are linked to the same RTGS account).
  
  - If an immediate liquidity transfer order cannot be settled, an alert is sent to the Payment Bank that initiated the transfer in line with the message subscription rules in the Common Static Data.

- **Pre-defined liquidity transfer order:**
  
  - Liquidity is transferred at a certain time or when a particular business event occurs, as defined by the account holder of the account or a T2S Actor with appropriate rights to debit the account.
  
  - The transfer is executed only once on the basis of a defined time or event.
  
  - Liquidity is transferred from a T2S DCA to an RTGS account only (either the specified transfer amount or “all cash” available in the T2S DCA will be transferred).
  
  - Any duly authorised T2S Actor may amend or delete the predefined liquidity transfer order.
Standing liquidity transfer order:

- Liquidity is transferred at a certain time or when a particular business event occurs, as defined by the account holder of the account or a T2S Party with appropriate rights to debit the account.
- The transfer is executed whenever the event in question occurs until the standing order is deleted.
- Liquidity is transferred from a T2S DCA to an RTGS account only (either the specified transfer amount or “all cash” available in the T2S DCA will be transferred).
- Any duly authorised T2S Actor may amend or delete a standing liquidity transfer order.

If insufficient liquidity is available on the accounts to be debited, T2S allows partial execution in the case of pre-defined/standing liquidity transfers. T2S allows a partial execution of an immediate liquidity transfer only if it is instructed to do so by a CSD acting on behalf of the Payment Bank.

As part of the business validation process, T2S checks that the content of immediate liquidity transfer orders (received from T2S Actors) or liquidity transfers (which have been generated from a standing or predefined liquidity order) is correct, and validates the consistency of the data contained in the immediate liquidity transfer received by T2S with the Common Static Data. A liquidity transfer which has been generated from a standing or predefined liquidity order is not validated by T2S.

After business validation, T2S communicates the acceptance/rejection of a liquidity transfer order to the Payment Bank and to the euro area or non-euro area NCB if the liquidity transfer order was sent from the RTGS system. In the event of failure or rejection, T2S sends a list of error/reason codes. T2S also communicates all changes in status of a liquidity transfer order.

After successful validation the liquidity transfer order is sent to the settlement functionality for processing. The booking function updates the balances on the DCAs involved on a gross basis. In the case of partial execution or of no execution, no further settlement is attempted. T2S communicates all changes in status of a liquidity transfer order in the course of its execution in accordance with the message subscription rules in the Common Static Data, and confirms all executed transfers between T2S and RTGS.
5.2 T2S SD.LIM 020: Limit management service

T2S provides the T2S Actor with different liquidity control mechanisms. A euro area or non-euro area NCB can control its parties’ T2S DCA by setting an auto-collateralisation limit for the T2S DCA. Payment Banks can also set different limits at the client level and monitor their utilisation. A Payment Bank can set up different limits for the liquidity provided to each of its clients, either against collateral or without collateralisation. Using T2S queries, the Payment Bank has a consolidated view of its client’s collateral holdings at any given point in time across multiple Security Accounts in either the same or different CSDs. The respective limits are automatically updated when used as a part of the settlement process. T2S performs validations to ensure that these limits are not breached. T2S does not allow cash movements between the Cash Payment Bank and its clients in T2S. The only cash in T2S is the cash on the DCA, which is in CeBM.

Euro area or non-euro area NCBs and Payment Banks can set and monitor the limits they provide to their clients.

- **External guarantee limit**: Cap on credit secured outside T2S that the Payment Bank sets for its client. The external guarantee limit and the unsecured credit limit are identical from the T2S viewpoint, except for the sequence in which they are triggered. Usage of the external guarantee limit is triggered before client-collateralisation.

- **Client-collateralisation limit**: Cap on the amount of credit extended against securities by a Payment Bank in T2S
Unsecured credit limit: Cap on the amount of credit granted by a Payment Bank (generally unsecured outside T2S)

Auto-collateralisation limit: Cap on the amount of credit extended against securities by a euro area or non-euro area NCB to the Payment Bank.

T2S ensures that all the required provision checks for the Payment Banks and their clients are performed simultaneously and that collateralisation operations are initiated on the basis of the results of the provision check. A Cash Payment Bank client’s credit exposure as well as the availability of sufficient headroom on different types of credit limits is determined solely on the basis of information available to T2S.

To prepare for client collateralisation, the T2S actor has to provide and to set up the information required for the link between its Security Account and its DCA, and to provide the necessary information for the Credit Memorandum Balance (CMB) Security Account Link Set and CMB Security Account Link7.

Furthermore, a T2S Actor can control the use of liquidity by reserving/ blocking cash for specific instructions. The amount of cash reserved/ blocked may not be used to settle instructions, unless the instruction being settled refers to the initial reservation/ blocking instruction.

5.3 T2S SD.LIM 030: End of day (EOD) cash management service

After the cut-off of settlement processing, the EOD processing is conducted in three steps. Information messages are sent to the initiating T2S Actor and other duly authorised T2S Actors in accordance with their message subscription preferences:

1. EOD release of unused cash restrictions:
   - All restrictions on cash (blocked cash, reserved cash) are released for the current Settlement Day.
   - New cash settlement restrictions regarding CoSD blocking are created for the next Settlement Day.

2. EOD release of auto-collateralised positions and transfer of cash balance:
   - The amount of outstanding auto-collateralisation is validated.

7 Further details can be found in the User Detailed Functional Specifications (UDFS), especially chapter 1.1.2 Liquidity management
- If there is no pending auto-collateralisation: No action is taken.

- If there are pending auto-collateralisation(s):
  - and the cash on the T2S DCA is sufficient to reimburse fully the pending auto-collateralisation, including possible cash rebalancing: T2S reimburses.
  - and there is insufficient or no cash on the T2S DCA to reimburse the pending auto-collateralisation, T2S:
    - checks for available cash via cash rebalancing from another DCA of the same T2S Actor;
    - releases the associated reverse (unwind) settlement instructions previously created;
    - creates instructions for positions that will not be released (equivalent to the pending amount of auto-collateralisation that cannot be reimbursed out of T2S), to transfer the collateral to the euro area or non-euro area NCB overnight collateral Security Accounts; and
    - rebalances the account to zero.

3. EOD liquidity transfer (cash sweep)

- Liquidity transfers are created for all T2S DCAs and the euro area or non-euro area NCB Account used for EOD reimbursement with non-zero cash balances.

- These liquidity transfers are settled in T2S and sent to the RTGS system.

5.4 T2S SD.LIM 040: Corporate action cash service

T2S enables a T2S Actor, receiving cash proceeds from corporate actions on its T2S DCA, to specify whether T2S should keep the cash proceeds on the T2S DCA or to retransfer them from the T2S DCA to the RTGS account (outside T2S) with which the T2S DCA is linked.

In such case, the T2S Actor must define a standing liquidity transfer order for the T2S DCA as part of the Common Static Data to be able to opt for an automated retransfer of cash proceeds to an RTGS account.

T2S allows the T2S DCA holders to use different T2S DCAs for the settlement of the cash leg of trading-related instructions and for the settlement of the cash leg of corporate action instructions.

During both the daytime Real-time settlement and night-time batch settlement T2S executes the standing liquidity transfer order as an immediate liquidity transfer to transfer the corporate action
proceeds to the RTGS account of the T2S Actor.

T2S also provides this setup and service for retransferring ‘monetary policy Repo’ related cash proceeds from a T2S DCA to an RTGS account.

5.5 T2S SD.LIM 050: Cash blocking and reservation service

T2S allows a T2S Party to use restrictions to block or to reserve a cash balance in a T2S DCA. For that purpose the CSD or the euro area or non-euro area NCB has to define the relevant restriction types as part of the Common Static Data.

Blocking a cash balance involves preventing the transfer of a specified amount of funds in a specific currency in one cash account to any other cash account by linking it to a specific purpose. Blocking in T2S never results in a negative cash balance, i.e. it is not possible to block an amount of funds greater than the available cash balance on a cash account.

Reserving a cash balance prevents the transfer of a specified amount of funds in a specific currency in one cash account to any other cash account except for the purpose for which the funds were reserved. The settlement of the underlying settlement instruction (for which the funds were reserved) results in the actual transfer of the reserved funds to another cash account and the subsequent removal of the reservation.

A T2S Actor may reserve a cash position without yet disposing of the required full amount of cash in that position. Any cash arriving in the reserved position will be attributed to the reservation until the required amount has been reached.

A T2S Actor may refer to an existing reservation/blocking in another settlement instruction, by referring to the unique reference number of the reservation’s/blocking. Such reference will be interpreted in such a way that the provisioning process includes the reserved/blocked amount of cash in its provisioning check. The reserved/blocked cash will be used first (ahead of unreserved/unblocked cash) for settlement of the instruction.

During business validation, T2S checks automatically whether one of these restriction types applies to the submitted settlement instruction or to an instruction for an intra-position movement to determine the further processing required. If the validation process finds a match for a restriction type, then the relevant restriction type is applied to the instruction.

5.6 T2S SD.LIM 060: Liquidity monitoring service

T2S provides different functions for monitoring the actual cash balances of the DCAs as well as the CMB limits to monitor the liquidity of the clients of the Payment Bank. T2S calculates the
amount of cash required for the settlement and informs the T2S Actor if more liquidity is needed.

Cash related queries allow duly authorised T2S Actors to obtain information about their account balance on the T2S DCA(s), outstanding intraday credit from auto-collateralisation, and potential liquidity based on securities on stock that can be used for auto collateralisation purposes. In addition, T2S provides information showing the overall liquidity.

A T2S Actor may request information on cash needs for instructions pending for settlement during the current Settlement Day, as well as cash forecasts for the following Settlement Day. Information on cash needs and cash forecasts covers T2S DCA liquidity needs.

Information for the on-going Settlement Day is intended to provide a snapshot of the cash required to settle instructions remaining unsettled at the moment of the snapshot. This information includes (as part of the cash required for the current day settlement) the value of potentially available auto-collateralisation.

Information on cash forecasts for the following Settlement Day and in particular for the following night-time settlement window is intended to allow T2S Actors to prepare and dedicate in advance sufficient cash for the settlement of their instructions during the following night-time settlement window. The cash forecasts are based on:

- cash needs resulting from the net balance between:
  - cash proceeds and
  - cash needs expected for settlements with the following day as the ISD; and
- the amount of intraday credit that can be obtained through auto-collateralisation;
- the amount of liquidity credit that can be obtained through external guaranteed limits and unsecured credit lines from Payment Banks or euro area or non-euro area NCBs.

Depending on the chosen report configuration, cash forecasts can be received as reports sent out automatically by T2S at certain points/when certain events occur during the Settlement Day. Preliminary information on cash can also be obtained via the query functionality.

However it should be noted, that these cash forecasts (received through the above-mentioned reports and via queries) are only indicative of the final cash needs, as the forecasts are based only on the information available in T2S: T2S does not take corporate action proceeds into account, if the relevant instructions are not submitted to T2S.

The T2S Actor has to be aware that these cash forecasts will change in the course of the
Settlement Day depending on new settlement instructions / liquidity transfers submitted to T2S. It is to be expected that the quality of the cash forecast will increase continuously during the day as additional settlement instructions and information become available in T2S.

A T2S Actor is able to define the floor and ceiling amounts per DCA in the Common Static Data. This functionality allows the T2S Actor to receive alerts if the amount of liquidity in the DCA reaches the minimum/maximum the DCA account holder has defined.

5.7 T2S SD.LIM 070: Multiple liquidity provider service

T2S DCA holders may receive liquidity from several RTGS accounts (i.e. from different liquidity providers) and use the proceeds in T2S. This cash can be transferred from the RTGS accounts prior to the start of Batch Settlement in T2S. Subsequently, a T2S DCA holder can use this cash for its own settlement purposes or to provide cash settlement services to its clients, during Batch Settlement in T2S.

At the end of the Batch Settlement, a T2S DCA holder may opt to establish liquidity transfers which will reimburse its different liquidity providers in the relevant RTGS systems with the remaining cash in the T2S DCA. This reimbursement facility is the “multiple liquidity provider” service.

The reimbursement of cash is executed via outbound liquidity transfers generated by T2S on the basis of the multiple “standing liquidity transfer order”. The priority of execution is defined by the T2S Actor in the “order link set” setup in the Common Static Data.

T2S validates whether a T2S DCA holder (liquidity receiver) has opted for a “multiple liquidity provider” service for reimbursement. If this is the case, T2S reimburses the liquidity providers in the sequential order of liquidity providers as set up in the order link setup (in the Common Static Data). T2S aims to reimburse each liquidity provider up to the maximum amount of the cash the liquidity provider transferred before starting to reimburse the next liquidity provider in the sequential order concerned. In the order link set, the main liquidity provider is setup as the last liquidity provider and therefore is the last liquidity provider to be reimbursed (assuming there is sufficient cash to reimburse all liquidity providers).
6 T2S SD-STD: Common Static Data Management Service Class

6.1 T2S SD-STD 010: Common Static Data management service

Common Static Data management is the service that T2S provides for setting up/inserting, changing/maintaining and inactivating/deleting Common Static Data in T2S regardless of the type of conceptual entity. T2S applies the same functional principles for inserting, maintaining and deleting all entities.

T2S processes all Common Static Data updates in real-time in both User-to-Application (U2A) and Application-to-Application (A2A) mode, except in the case of some preliminary functions which are only available in U2A mode. All Common Static Data entities are stored in the T2S database with a full audit trail and it is possible to query the actual occurrence of an entity as well as the historical data. Whenever a record in Common Static Data is changed, a new version of this record is stored including the timestamp and the identification of the T2S Actor performing the change, thereby maintaining a full audit trail.

T2S allows T2S Actors to parameterise the entities and the types of updates made by a T2S User or by a T2S process. In general, T2S will process these in real-time except during the Maintenance Window (see UDFS for further information). T2S checks for every change in a Common Static Data entity and for the change approval configuration for this entity and

---

8 The detailed list of available functions for the different modes are part of the UDFS and of the UHB.
processes the update in accordance with the configured parameters. The privileges of the
different T2S Users depend on the Common Static Data entity. Static security data changes made
by an automated interface do not require an independent change approval by a second user, but a
manual update by a person is subject to such approval (4-eyes principle).

T2S provides duly authorised T2S User with the functionalities to:

- identify all Static and Dynamic Data changes awaiting approvals;
- search for specific Static and Dynamic Data changes;
- search and display historic change information, including both approved and
  rejected changes; and
- approve and reject Static and Dynamic Data changes.

6.1.1 T2S SD.STD 011: Insert service component

T2S allows the duly authorised T2S User to insert a new occurrence of an entity into Common
Static Data. A T2S User is an individual or application that is allowed to communicate with T2S
when duly authorised and authenticated.

6.1.2 T2S SD.STD 012: Update service component

T2S allows duly authorised T2S User to update an existing occurrence of a Common Static Data
entity. T2S allow T2S Users to update occurrences of a Common Static Data entity if the
previous update of the same occurrence remains in the change approval queue. T2S prohibits the
concurrent update of occurrences of a Common Static Data entity. When a T2S User selects an
occurrence for editing, T2S locks the occurrence so that a second T2S User or T2S process
cannot access it for updating.

6.1.3 T2S SD.STD 013: Delete service component

When a duly authorised T2S User initiates the deletion of an occurrence in a Common Static
Data entity, T2S checks that there are no unsettled instructions and only zero positions pertaining
to that data. Only if that is the case will the deletion status of the occurrence be changed from
“active” to “deleted”. The deletion of an occurrence of a Common Static Data entity occurs only
logically.

The T2S archiving functionality is the only function which will physically delete an occurrence
of a Common Static Data entity from the active T2S database. The physical deletion of a
Common Static Data occurrence is only possible for logically deleted occurrences. To ensure the
referential integrity of data, Common Static Data occurrences are physically deleted from the
active database only after archiving processes have removed and archived the related
Transactional Data and position data as of a cut-off date that is determined by the retention plan. Data history and data revisions that took place before the archive date will be included in any physical deletion process even if the current record is still active - since the Transactional Data for which they are relevant would be removed by the archiving.

6.1.4 T2S SD.STD 014: Reactivate service component

In some instances, it is necessary to reactivate a logically deleted occurrence of Common Static Data. T2S allows duly authorised T2S Users to specify the Common Static Data entity and the identifier of an occurrence in that Common Static Data entity, and to reset the deletion status of an occurrence in that Common Static Data entity from “deleted” back to “active”.

6.2 T2S SD.STD 020: Securities Reference Data service

Securities Reference Data in T2S defines the set of entities and attributes that T2S requires for settlement and auto-collateralisation in CeBM.

The Securities Entity holds all attributes that exist only once for a security. Securities Reference Data require every security to have an ISIN code, compliant with ISO 3166. The creation of a new security will be effective immediately unless it requires dual entry approval. This also applies to updates of all attributes for the Securities Entity. Certain “non-standardised securities” that comply with all required criteria apart from not being fungible from a settlement perspective may still be entered in and processed by T2S.

The Securities Reference Data Service allows the CSD to create and maintain the Common Static Data of those securities for which it is the Securities-Maintaining Entity. In addition, the non-SME CSDs may maintain Market-Specific Attributes on securities for their market. The service allows the Issuer CSD to block or unblock ISINs both for itself and its Investor CSDs. T2S allows an Investor CSD to block or unblock ISINs.

6.3 T2S SD.STD 030: T2S Party data service

T2S deploys a flexible hierarchical party model to allow CSDs and euro area or non-euro area NCBs to manage their accounts and parties in an efficient way. The T2S Operator maintains the first and second level of the hierarchy. All other levels must be managed by the CSDs and the euro area or non-euro area NCBs respectively.

A T2S Party denotes any legal or organisational entity required in T2S as single legal entity to guarantee data segregation. The same legal entity, or organisational unit of a legal entity, may be set-up under several CSDs or euro area or non-euro area NCBs as a result of this principle. This entity includes the parties from the first three levels of the hierarchy model, the T2S Operator, the
CSDs, the participants of the CSD, the euro area or non-euro area NCBs and the Payment Banks. It also establishes the links between the different parties on the different hierarchical levels. A CSD can also be a T2S Actor for its own purposes defined in level 3 of the hierarchy as a CSD participant (see graph below).

T2S assigns each party a technical identifier, which the user can also use as the unique T2S Party code (participant code). T2S will use the BIC of a T2S Party to identify the T2S Party uniquely across in the euro area or non-euro area NCB - and CSD-specific reference data.

The CSD-part of this hierarchical structure contains all T2S Party data pertaining to securities settlement. The Security Account (on the lowest level of this part of the hierarchy) is assigned to the CSD participant and to the CSD. Some specific account types are assigned to level 2 parties, for example a Mirror account. Each CSD is responsible for maintaining the hierarchy including the Security Accounts of the different parties which are linked to it. CSDs assign and manage the access rights of their participants, including those of all their DCPs.

Security Accounts linked to the CSD participant and T2S DCAs linked to a Payment Bank form the lowest level of the hierarchy. The Security Accounts assigned to level 3 parties can for instance be omnibus accounts or DCAs. CSDs have access to euro area or non-euro area NCB party and account Common Static Data to link Security Accounts to T2S DCAs for the settlement of the cash leg of a settlement instruction. T2S will make available to the CSDs the relevant data for the linking of accounts without publishing all T2S DCAs. Access rights control which CSD is able to see the T2S DCAs needed for linking purpose. When a CSD sets up a Security Account, it can only see those T2S DCAs to which it can link a Security Account for settlement.

The euro area or non-euro area NCB part of the hierarchical structure includes all data relating to the euro area or non-euro area NCB and the T2S DCAs held with the euro area or non-euro area NCB by Payment Banks. In the third tier of this part of the hierarchy includes the Payment Banks.
which operate T2S DCAs to provide liquidity. The T2S DCAs are the lowest level of the hierarchy. The hierarchy links the T2S DCA to the relevant euro area or non-euro area NCB.

Euro area or non-euro area NCBs authorise the access to T2S DCAs by assigning the BIC of those parties, eligible for access to the cash account for settlement, to the T2S DCA. When entering a Security Account, the CSD only sees those T2S DCAs which have the same BIC assigned to them as the T2S Party that owns the Security Account.

6.4 T2S SD.STD 040: Security Account data service

Security Account reference data specify all information required for defining and processing a Security Account in T2S.

Security Accounts in T2S must be opened and closed by the CSD to ensure the consistency and integrity of Security Account reference data between the CSD and T2S. When the CSD opens an account, it must immediately trigger the opening of the relevant account in T2S. The same applies for the closing of an account.

T2S supports a T2S Actor - Security Account Relationship entity to specify a time-dependent relationship between a T2S Actor and a Security Account. The purpose of the entity is to allow a CSD in T2S to transfer a Security Account relationship from one account operator/sub-custodian to another account operator/sub-custodian within the CSD. The functionality enables a CSD to transfer an end-investor Security Account relationship from one account operator to another.

CSDs are also responsible for closing a T2S Security Account by setting the business status to “closed” and confirming the change. T2S only closes an account if:

- there is no un-settled instruction specifying the T2S Security Account for the
settlement;  

- the T2S Security Account is not part of an active T2S link set; and  
- there is no securities balance remaining on the T2S Security Account.

In case an unmatched instruction exists concerning an account that is closed, during the business revalidation the unmatched instruction is identified and will be cancelled.

### 6.5 T2S SD.STD 050: Cash account data service

The T2S DCA model specifies the requirements for assigning T2S DCA to Security Accounts for the settlement of the cash leg of settlement instructions. The T2S DCA entity specifies the T2S DCAs of Payment Banks in T2S. It also links the T2S DCA to the associated RTGS account concerned as well as establishing the reference link to the Payment Bank that owns the account and to the euro area or non-euro area NCB that operates the account.

The key responsibilities of each euro area or non-euro area NCB whose currency (euro and non-euro) is available for settlement in T2S are:

- set-up and maintain the DCAs of their RTGS participants for all securities-related payment transactions in their currency in T2S;  
- set up and manage Common Static Data, access rights and configuration data pertaining to its members and its own participation in T2S;  
- if required, provide for the interoperability of their own RTGS systems and collateral management systems with T2S;  
- if the euro area or non-euro area NCB chooses to participate in auto-collateralisation:  
  - to provide auto-collateralisation in its currency to its members in accordance with its self-defined eligibility criteria;  
  - if required, to provide to T2S, for the specific purpose of auto-collateralisation, a list of eligible securities and prices as well as any other data necessary for T2S to judge the eligibility of a specific security for a specific participant;  
- be responsible for the choice of its network provider(s) and to make every effort to maintain properly functioning connectivity to T2S functions properly.

Euro area or non-euro area NCBs are also responsible for closing a T2S DCA by setting the business status to “closed” and confirming the change. T2S only closes an account if:

- there is no unsettled instruction specifying the T2S DCA for the settlement of the cash
the T2S DCA is not part of an active T2S DCA link set; and
- there is no cash balance remaining on the T2S DCA.

The external RTGS Account Entity specifies all the external RTGS payment accounts to which an authorised T2S User can link a T2S DCA. This entity also provides the reference link to the Payment Bank that owns the account and the euro area or non-euro area NCB that operates the account.

The euro area or non-euro area NCBs have to add new external RTGS account for a Payment Bank or another euro area or non-euro area NCB in T2S. T2S assigns new external RTGS accounts an opened business status and the current Settlement Day as the opening date.

An external RTGS account can be closed by setting the business status to “closed” and confirming the change. T2S will not close an account if:
- there is an unsettled payment instruction specifying the external RTGS account;
- the external RTGS account has an active link to a T2S DCA; or
- the external RTGS account is defined in a current (not closed, not expired) standing liquidity transfer order.

T2S allows the blocking/unblocking of an RTGS account using T2S Actor and account settlement restrictions. The blocking of an RTGS account results in all T2S DCA linked to the account being blocking from settlement.

**6.6 T2S SD.STD 060: T2S User data service**

A T2S User is an individual or application that is allowed to communicate with T2S using a login name and certificate/smartcard and for U2A in addition an optional password and/or certificate for authentication. The assignment of the T2S User to a T2S Actor establishes the relationship between the T2S User and the system entity. T2S provides specific roles and privileges to restrict the access of this T2S User to business data of the CSDs and of the euro area or of the non-euro area NCBs.

T2S User maintenance defines the process of adding, changing and deleting users in T2S. Access to this functionality is restricted to system administrators only.

A system administrator is able to lock and unlock a T2S User without deleting the user by setting the attribute "lockout status" to "yes" or "no". If the system administrator assigns existing roles to or deactivates roles for a T2S User, T2S automatically assigns to the T2S User the privileges...
associated with that role.

6.7 T2S SD.STD 070: Roles and privileges data service

In order to comply with the principle concerning the separation of functions and roles, T2S implements roles and privileges as business concepts which refer to the right of T2S Actors to interact with T2S. Duly authorised system administrators configure roles and privileges to authorise other T2S Users to execute specific functions or view specific data.

A privilege is a right, either granted or denied, to execute certain functions within T2S, or to access and/or update certain data in T2S. It is through the privileges that access to functionality and data for specific roles is granted and restricted to T2S Actors. A privilege is uniquely identifiable, both internally in the application and to the T2S system administrator. Privileges are classified either as System privileges or Object privileges.

System privileges grant certain rights for a single or a homogeneous group of data objects. Object privileges grant rights in relation to a single or a group of Common Static Data objects.

The administrator grants a privilege by specifying whether (1) the associated functionality is allowed or explicitly denied; (2) the grantees of the privilege is allowed to grant the same privilege to another user or role; (3) the grantees of the privilege is allowed to use the function associated to the privilege in accordance with the two-eye- or four–eye-principles.

Account owners (i.e. a CSD or a euro area or a non-euro area NCB) may grant privileges to their clients, with different roles and privileges for each one. These roles and privileges can be differentiated by client and even among different accounts of the same client.

T2S privileges may for example grant:

- no access at all;
- read only access;
- the right to instruct with possible limitations concerning the type of instructions or the accounts to instruct on.

A role consists of one or more privileges. A CSD or a euro area or a non-euro area NCB may configure valid roles for its T2S parties as follows:

- If set up by the CSD, DCPs manage their T2S User administration.
- If set up by the euro area or by the non-euro area NCB, Payment Banks manage their T2S User administration.
Each CSD or a euro area or a non-euro area NCB needs to create and authorise a system administrator for each of its client T2S Actor of that CSD or of that euro area or of that non-euro area NCB. The system administrator is responsible for maintaining users and roles for this particular client. The CSD or euro area or non-euro area NCB administrator has to ensure, that the system administrator of the T2S Party has access only to those roles that the CSD or euro area or non-euro area NCB permits. Accordingly, T2S enables each CSD or the euro area or the non-euro area NCB to grant its clients access to a different set of roles, depending on the services provided by the CSD or the euro area or the non-euro area NCB to each T2S Party.

CSDs or euro area or non-euro area NCBs participating in T2S must continue to comply with Legal and Regulatory Requirements. T2S therefore allows the configuration of CSD- or euro area or non-euro area NCB - specific roles. The CSDs or euro area or non-euro area NCB may differentiate the access they grant to T2S services and functions on the basis of the Legal and Regulatory Requirements to which they are subject.

6.8 T2S SD.STD 080: Restriction management service

T2S must support the T2S Operator, CSDs and euro area or non-euro area NCB by enabling them to provide specific validations and processing of settlement instructions to fulfil the Legal and Regulatory Requirements and the supervisory requirements in the markets that they service. T2S therefore allows the T2S Operator, CSDs and euro area or non-euro area NCBs to define their own restriction types.

Restriction types are attributes that define the specific processing characteristics for a securities position, cash balance, Security Account, T2S DCA, T2S Party or settlement instruction to ensure configurability of specific requirements, as prescribed by national Legal and Regulatory Requirements and practices, and to avoid hard-coding in the application software.

T2S provides the following restriction processing types:

- Blocking – blocks an instruction from settlement;
- Rejection – rejects an instruction at validation;
CSD Validation Hold – accepts a settlement instruction at validation (not applicable to settlement restrictions) but holds it for a subsequent release by the CSD⁹;

Reservation – reserve a cash balance or securities position;

Balance Type / Earmarking – define and manage position types for securities and balance types for cash balances.

Restrictions can also be defined as either a positive or negative parameter set and in time (from and to).

During the validation process, T2S automatically verifies whether one of the defined restrictions applies to the instruction submitted.

A T2S User may define specific rules for restriction types. These define the sequence in which T2S applies a logical set of parameters to determine whether a specific restriction applies to the instruction. The restriction matrix defines the specific parameter values within a rule. T2S stores matrix entries for a rule in a rule set. A matrix entry defines an occurrence of a valid set of values, specifying the actual criteria against which T2S must validate a settlement instruction to determine whether a restriction type applies.

T2S allows duly authorised users to

- add new rules for a restriction type;
- (re-) define the sequence of rules for a restriction type;
- delete rules for a restriction type if the user has deleted all occurrences under that rule; and
- add and delete matrices in a rule.

This functionality is also used by CSDs to define which settlement instructions will be put on CSD Validation Hold. It allows CSDs to execute certain tasks / validations locally prior to the settlement of the underlying instruction.

---

⁹ Further details for the CSD validation hold are provided in the User Detailed Functional Specifications (UDFS) chapter 1.1.1 Settlement
6.9 T2S SD.STD 090: Attribute domain data service (market-specific attributes)

Attribute domains in T2S provide the valid list of values allowed for an attribute (table column or a data field in physical terms). They include a list of all the valid values that a user can enter for an attribute of a static or Transactional Data entity. T2S uses attribute domains for field validations and for documenting the business definition of a value in an attribute.

T2S provides a general Common Static Data component that allows the duly authorised T2S User to logically create, modify and deactivate market-specific attribute domains, on the basis of the existing data definitions (attributes). These market-specific attribute domains allow the T2S Operator, CSDs and euro area or non-euro area NCBs to define their own restriction types as described above. T2S allows the definition of additional values, mapped to an attribute.

T2S limits the actions that a user can trigger in the database using attribute domain management. T2S allows the registration and deactivation of attribute domains using pre-defined database tables.
7 T2S SD. INF: Information Management Service Class

7.1 T2S SD.INF 010: Status management services

As part of its settlement services, T2S maintains the settlement statuses of any instruction it processes. T2S informs duly authorised T2S Actors of the result of all settlement services and of all changes to the statuses of instructions, depending on the message subscription chosen by the T2S Actor.

T2S provides multiple-statuses reporting that gives more flexibility and brings more efficiency than single-status reporting. In this context, T2S provides the values of the different statuses for each instruction in a report or query response. Status messages report the status that has changed. If instructions are rejected, settlement attempts unsuccessful or instructions cancelled, T2S also informs the relevant T2S Actor why this has happened.

7.2 T2S SD.INF 020: Report generation service

T2S provides a defined set of reports. Reports are triggered automatically by T2S. All reports are available in both User-to-Application (U2A) and in Application-to-Application (A2A) mode as in the T2S Connectivity Services description. These reports are not, and should not, be considered as Regulatory Reports. T2S Actors may use the query services described hereafter to receive the necessary information from T2S to provide their regulators with the required information.

T2S reports are either event-triggered or sent at a fixed time. When a CSD, T2S Actor or euro area or non-euro area NCB require information at a time not so triggered, the information can also be retrieved using the query service.

Reports containing information either on individual accounts or on a set of accounts can be sent
to the relevant CSDs and DCPs, or to the relevant euro area or non-euro area NCB. T2S reports
are based on the latest available data and contain a date and time stamp. In addition, T2S sends
successive versions of defined reports with the information that changed from the previous
version to the next version of that report (delta reporting). The additional information includes
the attributes of the reported items as provided in the previous version of the report.

A DCP may receive reports only on:

- its own securities and cash balances, those of its clients and those of any other T2S
  Actor for which the appropriate authorisation was granted;
- instructions that were submitted by the T2S Actor (or a Third Party with access rights -
supported by power of attorney to do so on behalf of the T2S Actor) and instructions
  that refer to the securities or cash account of the T2S Actor (or any sub-account thereof);
- its own Common Static Data, as well as some generic Common Static Data on
  instruments and the daily schedule.

A CSD may receive reports only on:

- instructions that were submitted by the CSD in T2S itself, its DCPs, or by its
  participants;
- securities transactions and balances of the CSDs own accounts in T2S, those of its
  DCPs and those of its participants; and
- Common Static Data of the CSD in T2S itself, its DCPs, and of its participants, where
  privileges permit. These Common Static Data include those ISINs for which the CSD
  acts as Security Maintaining Entity (SME)\textsuperscript{10}. Additionally, a CSD may query all
  Common Static Data that relate to its admission rule, for securities as well as for parties.

A euro area or non-euro area NCB may receive reports only on:

- instructions that were submitted by the euro area or non-euro area NCB in T2S itself, or
  by its Payment Banks;
- cash balances of its own DCAs in T2S and those of its Payment Banks as well as cash
  movements on its own DCAs and those of its payment banks; and

\textsuperscript{10} Further details can be found in the Manual of Operational Procedures (MOP)
1377  ▪ Common Static Data of the euro area or non-euro area NCB in T2S itself, and of its
1378  Payment Banks. Additionally, a euro area or non-euro area NCB may query all Common
1379  Static Data that relate to its national currency.
1380
1381  A Payment Bank may receive reports only on:
1382  ▪ instructions that were submitted by itself;
1383  ▪ cash balances of its own DCAs in T2S; and
1384  ▪ its own Common Static Data, and that pertaining to its DCAs.
1385
1386  T2S provides the following report types (non-exhaustive, a full list can be found in the UDFS):
1387  ▪ Statements of holdings;
1388  ▪ Transaction reports:
1389    o Statement of transactions;
1390    o Statement of pending instructions;
1391    o Statement of settlement allegements;
1392    o Statement of Security Accounts at EOD;
1393    o Statement of changes to Common Static Data; and
1394    o Billing data report.
1395
1396  ▪ Cash forecast reports:
1397    o Current Settlement Day cash information; and
1398    o Following Settlement Day cash forecast.
1399
1400  **7.3 T2S SD.INF 030: Query service**
1401
1402  T2S allows information to be queried in T2S. Queries are triggered by the duly authorised T2S
1403  Actor. All queries are available in User-to-Application (U2A) and a subset is available in
1404  Application-to-Application (A2A) mode (see UDFS for further detail). All securities instructions,
1405  and balances and Common Static Data queries are available for all CSDs in T2S, DCPs as well as
1406  euro area or non-euro area NCBs and Payment Banks, in accordance with to the access rights.
1407
1408  T2S accepts all queries at any point in time during T2S opening days. T2S processes all queries
1409  in real time, on the basis of the latest available data. During the night-time settlement sequences,
1410  T2S queues balance queries sent in Application-to-Application mode while the U2A balance
1411  queries will not be processed. T2S responds to the A2A queries at the end of each sequence
inside a cycle with the latest position.

T2S provides standard queries which can be taken as the basis (blueprint) for individual, non-
standard queries. For individual, non-standard queries, T2S provides the option of specifying
parameters in the query to fulfil the needs of the querying T2S Actor. When processing queries,
T2S takes into account all access rights as defined in the Common Static Data. T2S will only
return results where the T2S Actor that has submitted the query has the right to access the
underlying data. CSD/ euro area or non-euro area NCB and T2S Parties may act as service
providers for indirect Parties or e.g. remote brokers.

7.3.1 T2S SD.INF 031: Query service for T2S Actor service component

A T2S Actor may query the following – subject to access rights:

- its own securities positions;
- instructions submitted by the T2S Actor itself (in case of direct connectivity), or by a
  Third Party that has access rights in T2S supported by a power of attorney; and
- its own Common Static Data, as well as some generic Common Static Data relating to
  e.g. instruments and the daily schedule.

7.3.2 T2S SD.INF 032: Query service for CSDs service component

A CSD in T2S may query the following:

- instructions that were submitted by the CSD itself, or by its DCPs;
- securities and cash balances of DCA(s) of the CSD itself and of its T2S parties in T2S;
- Common Static Data of the CSD itself, and of its T2S Actors;
- Common Static Data pertaining to securities.

7.3.3 T2S SD.INF 033: Query service for euro area or for non-euro area NCBs service
  component

A euro area or non-euro area NCB in T2S (acting in its role as euro area or as non-euro area
NCB) may query:

- cash balances of the DCAs kept at the euro area or the non-euro area NCB in question;
- movements on the DCAs kept at this euro area or this non-euro area NCB; and
- Common Static Data pertaining to the DCAs for which it is responsible.

Additionally, a euro area or a non-euro area NCB may act as a T2S Actor of a CSD. In this case,
the euro area or the non-euro area NCB has the same access rights as any other T2S Actor.
Finally, if a euro area or a non-euro area NCB plays the role of a CSD, that euro area or non-euro area NCB, when doing so it has the same access rights of a CSD.

7.3.4 T2S SD.INF 034: Query service for Payment Banks (liquidity providers) service component

A Payment Bank in T2S (acting in its role as liquidity provider) may query:

- cash balances of its DCAs; and
- Common Static Data pertaining to the DCAs for which it is responsible.

7.3.5 T2S SD.INF 035: Settlement-related queries service component

During the night-time settlement cycles, T2S stores balance queries sent in Application-to-Application (A2A) mode, then replies with a message that T2S is currently running a cycle and that T2S will respond to the query at the end of the cycle with the latest position.

T2S provides different standard queries related to settlement:

- Securities balance query:
  - The Securities Balance Query returns an account view on the position at a particular point in time, the latest securities position or at the close of settlement if requested after close of settlement, all positions are summarised in the account structure that is compatible with the query parameters.
  - The Securities Balance History Query returns all positions that occurred during a particular time period, all positions are summarised in the account structure that is compatible with the query parameters.

- Settlement instruction query:
  - T2S allows T2S Actors to query settlement instructions in accordance with the Actor’s roles and privileges.
  - T2S provides a settlement instruction status audit trail query which allows a T2S Actor to query settlement instructions on the basis of the business processing status or a combination of business processing statuses on a specific date or in a specific period in the past.

7.3.6 T2S SD.INF 036: Cash balance-related queries service component

In accordance with their access rights, euro area or non-euro area NCBs and settlement/ Payment Banks may query:

- the current balance of one or more T2S DCAs;
- the total current collateral value of securities earmarked and available (on stock) for auto-collateralisation for a T2S DCA. The collateral value of securities, calculated by the query, does not include securities on flow, as the settlement process will use these automatically;
- for a specific T2S DCA, the current total collateral value of every security, earmarked and available (on stock) for auto-collateralisation, in all Security Accounts, linked to the T2S DCA for settlement of the cash leg. The collateral value of securities, calculated by the query, does not include securities on flow, as the settlement process will use these automatically;
- the amount of outstanding intraday credit stemming from auto-collateralisation, defined as the difference between the credit utilised and the credit reimbursed;
- for a specific T2S DCA, the collateral (amounts and securities) utilised for outstanding intraday credit stemming from auto-collateralisation;
- the total collateral (amounts and securities) utilised for outstanding intraday credit stemming from auto-collateralisation.

In addition to the queries described above, T2S provides some screens in the T2S Interface (U2A mode) which give a consolidated view of the balances available on the different DCAs of each Payment Bank to facilitate the liquidity management of the treasurer(s) at the Payment Bank itself. These screens are available to directly connected Payment Banks and their euro area or non-euro area NCB (further detailed in the User Handbook and the documentation on the GUI interface).

In order to manage the liquidity of their DCAs, euro area or non-euro area NCBs and their Settlement/Payment Banks may also query:

- limits and their utilisation,
- liquidity transfer orders, and
- liquidity transfer orders for multiple liquidity providers.

A CSD in T2S may query the cash balances of its own DCA(s) and those of its T2S parties in T2S.

7.3.7 T2S SD.INF 037: Common Static Data-related queries service component

Common Static Data queries are related to all main entities in Common Static Data. CSDs and CSDs’ participants may query Common Static Data in accordance with their access rights.

T2S also provides a Common Static Data audit trail query which allows a T2S Actor (in
accordance with its access rights) to query all revisions to an occurrence of Common Static Data.

Standard Common Static Data queries allow the T2S Actor to query, in accordance with its access rights:

- Security reference data
- T2S Actor reference data
- Security Account reference data
- T2S DCA reference data
- T2S calendar and diary/daily schedule
- T2S entities
- Attribute domains
- T2S Actors, roles and privileges
- Restrictions
- Currency reference data
8 T2S SD. CON: Connectivity / Communication Service Class

T2S does not provide technical connectivity/network services between the T2S Actors and T2S among its services. Network services have to be procured by the T2S Actors directly from one or more of the accredited Network Service Providers (NSP). T2S defines the technical and operational requirements for the NSPs. 11. NSPs offer a catalogue of services with appropriate solutions for high settlement volume and small settlement volume T2S Actors. The Connectivity Service catalogue contains the connectivity to T2S service NSPs provide and the additional services offered by these NSPs, including:

- detailed services;
- service levels, detailing performances, availability and support commitments;
- volume related services;
- dedicated connectivity solutions; and
- backup/alternative network access solutions.

---

11 The T2S Connectivity Guide provides further details on the different roles and responsibilities regarding the Connectivity Services
8.1 T2S SD.CON 010: Messaging services

T2S provides standard, time-event-driven and business-event driven messages based on and compliant to the largest extent possible with the ISO 20022 / UNIFI (Unified Financial Industry Message Scheme) standard. Communication between T2S Actors and T2S has to comply with the formats and specifications defined in T2S. T2S supports push and pull mode for files and single messages in Application-to Application mode (A2A), as well as a Graphical User Interface (GUI) in User-to-Application mode (U2A).

In T2S “business terms” a message is a single instruction (e.g. a settlement instruction, matched or unmatched, a Common Static Data maintenance instruction, etc) and in “technical terms” an XML string that refers to one or more “business messages”.

In T2S “business terms” a file is a set of instructions (more than one) and in “technical terms” a XML string that refers to one or more “business messages”, possibly of different types. Its size should be within a defined range (minimum and maximum considering performance aspects).

For each message or file received by T2S an acknowledgement is sent to the sending T2S Actor. An acknowledgement from the receiving T2S Actor is also expected for each message or file T2S sends out. Security-settlement-related and cash-management-related messages follow the same logic.

Inbound and outbound traffic is stored in T2S in original format messages (before any transformation) and the messages are kept with time-stamping information and signature.

8.1.1 T2S SD.CON 011: Push messaging service component

During the Real-time Settlement T2S sends real-time standard messages to the T2S Actors which are triggered by the relevant business events. These events for the generation and subsequent sending of the different messages are described in the corresponding chapters of this Service Description.

After each cycle of the Batch Settlement T2S sends settlement related messages to the T2S Actors. For a given instruction only the most recent valid statuses will be sent. Only settlement-related messages resulting from a night-time settlement sequence are bundled into a file.

Copies are available for a subset of messages and can be received upon subscription by the relevant interested parties (a full list can be found in the UDFS).

T2S message subscription is a service that allows a CSD or another duly authorised T2S Actor with direct connectivity to T2S to subscribe to copies of messages sent between a Directly Connected Party (DCP) and T2S in real-time using push mode messaging.
The T2S Actor must define in Common Static Data message subscriptions for all messages they want to receive. T2S only sends those messages the T2S Actor has subscribed to, there are no mandatory messages apart from the technical acknowledgements, query responses and inbound processing errors (a full list can be found in the UDFS), which are always delivered to the sender of the message. All messages, which are used by T2S, are available for message subscription. T2S will not send any message not subscribed to beforehand, although T2S generates all messages in accordance with the business context.

Subscriptions are based on one or more of the following parameters:

- Message type
- Instruction type
- Instruction status
- Participant
- Account
- ISIN

For euro area or non-euro area NCBs, the messaging service includes i.a.:

- messages for each utilisation of intra-day credit stemming from auto-collateralisation;
- and
- messages for each repayment of intra-day credit stemming from auto-collateralisation.

The message subscription rules are defined and maintained in the Common Static Data by the T2S Actor.

**8.1.2 T2S SD.CON 012: Pull messaging service component**

T2S Actors may request to receive specific messages from T2S. T2S uses this mode mainly for query services and reports. Additionally, through the Graphical User Interface (GUI) the T2S Actor may pull queries and reports.

**8.2 T2S SD.CON 020: Technical validation services**

T2S verifies that all inbound communication (messages and files) is compliant with T2S required syntax, format and structure. The message and file integrity check is part of the validation and ensures that only messages and files from T2S Parties enter the T2S applications. T2S validates files using the same standard as for the messages and ensures that inbound files are not lost, that outbound files are neither lost nor duplicated and that the recommendations of the Giovannini file
transfer rulebook are applied (generic rules for file construction and best practices for file transfer operations for any and all file transfers, on any network).

If there are structure problems in a received message, T2S rejects the message. If there are file transfer or structure problems inside the file, T2S rejects the file in its entirety. If there are validation problems at the level of individual instructions within the file, the file is normally processed and a rejection message is sent for each individual invalid instruction the file contains.

T2S verifies whether the communication was received from a secured and recognised technical address configured in the Common Static Data.

8.3 T2S SD.CON 030: Connectivity types services

8.3.1 T2S SD.CON 031: Application to Application (A2A) service component
Application to Application (A2A) mode in T2S is a connectivity mode to exchange information between the T2S software application and application at the T2S Actor. In T2S, A2A can be based on either XML messages or file transfer. The ISO 20022 standard is applied as far as possible, for both inbound and outbound communication.

8.3.2 T2S SD.CON 032: User to Application (U2A) service component
The duly authorised T2S User can communicate with T2S via a web based Graphical User Interface (GUI), a connectivity mode to exchange information between software application of T2S and a T2S Actor and which is the User-to-Application interface (U2A) for interaction with T2S. The roles and privileges assigned to a T2S User determine which functions this user may execute and which data this user is allowed to see and to maintain.

8.4 T2S SD.CON 040: Information security management services
Information Security management services are a crucial part of the total package of T2S services, in terms of confidentiality, integrity and availability as well as authentication, accountability, non-repudiation and reliability of the T2S information.

Confidentiality or non-disclosure agreements between T2S and the T2S Actors address the requirement to protect Confidential Information using legally enforceable terms. Any access to the service’s information by external parties must be controlled. Where there is a business need for working with external parties that may require access to the service’s information, or when a product or service is obtained from or supplied to an external party, a risk assessment is carried out to determine Information Security implications and control requirements.
Access by external parties to the service’s information is not provided until the controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement.

8.4.1 **T2S SD.CON 041: Authentication service component**

Authentication is a security mechanism which verifies the identity of an individual T2S Actor (the T2S User) or application trying to connect to T2S. A T2S User is an individual or application that is allowed to communicate with T2S using a login name and certificate/smartcard and for U2A in addition an optional password and/or certificate for authentication.

T2S supports different types of authentication:

- Simple authentication requires the T2S User to enter the T2S User ID and the respective password only. This is applicable only for U2A.
- Simple Certificate authentication requires the T2S User to use a certificate without entering a password in T2S. This is applicable only for A2A.
- Advanced Certificate authentication requires the T2S User to use a certificate in addition to entering the T2S User ID and respective password in T2S. This is applicable for U2A only.
- Smartcard authentication requires the T2S User to identify himself to the system using a smartcard in addition to entering the T2S User ID and respective password.

T2S stores and manages certificates as part of the Common Static Data. For every inbound communication T2S verifies:

- the identification of the sender;
- whether the digital signature of the inbound communication corresponds to the certificate of the sender;
- the T2S Actor technical address;
- the network service used for the communication; and
- if the sender information of the inbound communication is defined in the Common Static Data.

8.4.2 **T2S SD.CON 042: Authorisation service component**

Authorisation is a security mechanism which verifies that a T2S User or application (trying to connect to T2S) has the appropriate privilege to access certain functions or data within T2S. Authorisation is managed via the roles and privileges assigned by the T2S system administrators.
Initially the CSDs and the euro area or the non-euro area NCBs (with respect to the Payment Banks) grant and manage the authorisation. Within a DCP or a Payment Bank, a system administrator may grant additional authorisations which are limited by the authorisation granted to the T2S Actor by the CSD or euro area or non-euro area NCB.

T2S verifies the authorisation for every service and data access requested by a T2S User.

8.4.3 T2S SD.CON 043: 4-eyes principle service component

T2S ensures that any T2S operation to be executed in 4-eyes-mode is confirmed by a second authorised T2S User. The 4-eyes principle is only possible for U2A communication.

When a T2S User changes any occurrence of Static or Dynamic Data, which is subject to independent approval, T2S creates the changed version of the data as a new occurrence in the relevant revision entity and accords it a status "awaiting approval". The current version remains unchanged and is used until an independent source approves the update. If the independent approver accepts the change, T2S accepts the update and gives it the status "approved" in the Common Static Data entity. T2S retains the previous version of the data from the current entity as part of the audit trail in the revision history.

If the update is not approved, T2S updates the status of the change to "rejected" and it remains as an unapproved change in the revision history.

8.5 T2S SD.CON 050: Message sequencing services

T2S assigns each outgoing message a business sequence number which allows all T2S Actors to identify the sequence of messages T2S has sent. The receiving T2S Actors can thus identify whether messages are missing or misplaced in the sequence.

This service is used for all business related messages sent out by T2S.

8.6 T2S SD.CON 060: Direct connectivity services

Direct (technical) connectivity is a technical facility which allows T2S Actors to access T2S and use its services without using the relevant CSD/ euro area or non-euro area NCB as a relay or proxy. Direct connectivity affects neither the business or legal relationships between CSD and T2S Actor, nor the processing of the instructions of the CSD’s or euro area or non-euro area NCB’s T2S Actor.

Direct connectivity is a technical concept and means the existence of a (direct) network connection between a T2S Actor and T2S. It does not mean that the T2S Actors concerned has any particular roles or privileges.
DCPs have to be certified to participate directly in T2S. The relevant CSD or euro area or non-euro area NCB (i.e. the one the DCP is a participant or member of) has to ensure that the DCP fulfils all relevant conditions for participation of the DCP in T2S. T2S ensures that each DCP receives services as authorised by its CSD or by its euro area or non-euro area NCB, and the same Service Levels. Furthermore, T2S ensures that no connected system can harm T2S or any other connected system. Before being able to access the T2S production environment, both the CSD / euro area or non-euro area NCB and its DCP(s) therefore have to successfully pass a series of mandatory tests.

An individual T2S Actor may wish to participate as a DCP in more than one CSD or euro area or non-euro area NCB. In such case, the T2S Actor is deemed to be a separate DCP within each CSD or euro area or non-euro area NCB, and thus has a DCP account and related contractual arrangements with each of the CSDs or euro area or non-euro area NCB concerned.

### 8.7 T2S SD.CON 070: Routing services

T2S allows duly authorised T2S Actors to configure routing information which T2S uses to deliver outgoing messages to them. Each T2S Actor can set up several routing conditions and each routing condition includes the network service and the technical address. T2S identifies the T2S Actor entitled to receive the message on the basis of on the configuration in the Common Static Data, namely:

- the message subscription preference of the recipient; and
- the technical address to which the message should be routed (when there are multiple technical addresses, the first technical address (according to priority) is chosen).

T2S ensures that outbound messages will be routed to the appropriate technical address of the receiving T2S Actors.

T2S sends a message as a direct response upon receipt of a message, It sends the message to the T2S Actor’s technical address, which was used to send the underlying message, rather than the address defined in the Common Static Data.
9 T2S SD. SUP: Operations and support service class

To ensure service support and delivery in accordance with agreed Service Levels, T2S uses predefined processes based on the proven Information Technology Infrastructure Library (ITIL) concept. ITIL provides a set of best practices for managing information technology (IT) infrastructure, development, and operations.

T2S Service delivery is coordinated through the operations and support services and the required activities and processes are delivered and managed in accordance with agreed Service Levels for T2S.

9.1 T2S SD.SUP 010: T2S Business Application configuration services

T2S ensures the continuous management of its configuration.

9.1.1 T2S SD.SUP 011: T2S Calendar service component

For settlement of transactions against payment/delivery and/or free-of-payment/delivery in euro or non-euro CeBM, a common calendar is defined in the Service Level Agreements, as followed by all euro area markets.

During weekends, after the end of the Friday Settlement Day, T2S moves to the Settlement Day of the following Monday and performs the related activities until the end of the night-time
settlement period. On the Monday, T2S starts with the preparation of day-time settlement as the
continuation of the same Settlement Day.\textsuperscript{12}

\textbf{9.1.2 T2S SD.SUP 012: T2S Settlement Day service component}

T2S operates on a single harmonised timeframe for centralised settlement procedures in euro and
non-euro CeBM. This timeframe represents a balance between the user requirements for a pan-
European timetable and the constraints and business needs of existing local schedules, and is in
accordance with the market’s request for harmonised post-trading practices in the EU.

T2S settlement services are available continuously during the night-time and the day-time
settlement periods except for a short period during the Maintenance Window. T2S does not
perform any settlement services outside the night-time and day-time settlement periods.

The change of the T2S settlement date defines the start of a new Settlement Day. Following the
change of the Settlement Date:

\begin{itemize}
  \item T2S validates settlement instructions against Common Static Data valid as of the new
    settlement date and resulting from validated changes to the Common Static Data; and
  \item T2S settles instructions on the new settlement date.
\end{itemize}

The following is an overview of the T2S Settlement Day. A detailed description including time
lines can be found in the T2S Manual of Operational Procedures (MOP):

\begin{itemize}
  \item The T2S Settlement Day begins with a start-of-day (“SOD”) period, starting after the
    change of the settlement date and ending prior to the start of night-time settlement. It
    includes processes that are critical for the smooth preparation of the night-time
    settlement procedures, such as the identification and revalidation of eligible instructions
    and changes to the Common Static Data valid as from or as for this settlement date.\textsuperscript{12}
    During this period liquidity transfers from RTGS systems will be accepted.
  \item The following night-time settlement period starts after the end of the “SOD” period and
    ends prior to the Maintenance Window. During the night-time settlement period mainly
    settlement instructions that were input on previous Settlement Days with an Intended
    Settlement Date that corresponds to the current settlement date are processed. The night-
    time settlement period consists of two settlement cycles.
\end{itemize}

\textsuperscript{12} Additional detail and further rules regarding the T2S calendar can be found in the Manual of Operating Procedures (MOP)
After the night-time settlement period the T2S schedule includes a technical window for system maintenance.

After the end of the Maintenance Window T2S starts the day-time settlement period, which is used mainly for T+0 (same-day or intraday) settlement. In addition, it is during this period that failures from night-time settlement can be resolved.

Before the End-of-Day (EOD) period starts, T2S operates different cut-off times for DvP, FoP, euro area or non-euro area NCB operations.

The EOD period of T2S starts after the end of the day-time processing and finishes prior to the change of the settlement date, permitting CSDs and their participants to perform critical end-of-day activities, such as fulfilling reporting requirements. From the start of the end-of-day procedure, securities and cash positions are stationary (with the exception of EOD procedures related to the auto-collateralisation as described above) since no settlement can occur until the start of the next Settlement Day’s night-time settlement period.

### 9.2 T2S SD.SUP 020: Operational monitoring services

The T2S Operator monitors the T2S infrastructure and the T2S Business Application continuously:

- The T2S Operator observes the behaviour of the T2S production environment. If deviations from the normal Settlement Day are detected (the normal Settlement Day being defined as the behaviour of T2S over a defined time period):
  - within defined boundaries, the T2S Operator can trigger the appropriate corrective actions, when required; and
  - if necessary, the T2S Operator raises the alarms and indicates the appropriate level of priority as quickly as possible.

- In the event of operational issues the T2S Operator cannot resolve, the T2S Operator reports aggregated up-to-date monitoring information.
  - In Crisis and contingency situations, the T2S Operator provides up-to-date and comprehensive information to the crisis manager.

---

13 See further details in the SLA and in the MOP
In the event of an incident or problem, the T2S Operator provides and tracks information about the status and logs its history, as well as documenting the analysis and solution.

- The T2S Operator reports his activities to assist in the Service Performance Indicators reporting required for Service Information and monthly Service Level Agreement reporting.

### 9.3 T2S SD.SUP 030: Business continuity management services

Business continuity in T2S is understood to mean managing single component failures as well as failures of a single site without losing data. The Business Continuity Management service ensures that the required IT technical and services facilities (including computer systems, networks, applications, telecommunications, technical support and Service Desk) can be recovered within required, and agreed, business time-scales.

The technical environment for the T2S data centre and application follows the “two regions / four sites” architecture. Inside a region, the distance between the two sites is more than 10 kilometres. System and application software are kept updated in parallel at the four sites and each of the four T2S sites satisfies the agreed Service Levels.

Different mechanisms and procedures are implemented to guarantee business continuity:

- **Single component failure**
  - Hardware/Software and telecommunication components redundancy
  - Software quality control and test execution
  - Operational procedures (e.g. Change and Release Management)

- **Site failure**
  - Data in the two local sites are mirrored synchronous
  - Local recovery procedure to restart on alternate site

### 9.4 T2S SD.SUP 040: Disaster recovery and crisis management services

Disaster recovery services in T2S are understood to mean ensuring the resumption of T2S Services which were discontinued due to a high-impact disruption of normal business operations affecting a large metropolitan or geographic area and the adjacent communities that are economically integrated with it.
In addition to impeding the normal operation of financial industry participants and other commercial organisations, major operational disruptions typically affect the physical infrastructure.

Disaster recovery services ensure that the T2S Services can be recovered in an alternate region within the times defined in the Service Level Agreement. The T2S Business Application is installed in two separate regions and the data in the two regions are mirrored in asynchronous mode. Regional disaster recovery procedures are defined to restart the solution and the applications in the alternate region. Additionally, T2S uses a “periodical rotation” procedure to ensure that all staff are properly trained and both regions are capable of hosting the T2S Services. T2S has defined a crisis management process to coordinate all activities in Crisis Situations. The crisis management process guarantees effective coordination of activities within all the involved organisations and appropriate communication, i.e. early warning and clear instructions to all concerned, if a Crisis occurs.

9.5 T2S SD.SUP 050: Archiving services

T2S provides a central archive for its own purposes covering a 10-year period. The T2S central archive includes T2S static and Transactional Data.

T2S archives immediately all incoming and outgoing messages and files in their original format. After three months, T2S archives all instructions (settlement instruction, cash movements) as well as Common Static Data, billing and audit data. In order to ensure the integrity of static and Transactional Data, Common Static Data revisions and Common Static Data history remain in the operational databases until the archiving procedures moves the Transactional Data that reference it into the archiving database.

CSDs, euro area or non-euro area NCBs and T2S Operators have direct access to archived data via A2A or U2A interfaces. Provided it is duly authorised by its NCB, a DCA holder has direct access to archived data of relevance to it. Other T2S parties have to request their CSDs to retrieve and provide archived data to them.

9.6 T2S SD.SUP 060: T2S service desk services

T2S service desk provides a single, central point of contact for the CSDs, euro area or non-euro area NCBs, DCPs (if so authorised by their CSD), or DCA holders (if so authorised by their euro area or non-euro area NCB) for handling all incidents, queries and requests related to business, functional or technical issues related to T2S. The T2S service desk is accessible 24 hours a day
on T2S operating days. The Service Levels differ depending on the time of day.

On the basis of the complexity level of the service request/enquiry, the T2S service desk guarantees different response times, in accordance with the response time matrix as published in the Service Level Agreement. Service Levels are measured against this matrix. All enquiries are recorded, and confirmations are provided to CSDs, euro area or non-euro area NCBs or DCPs (if duly authorised by their CSDs) when service requests are received.

T2S has ITIL-based problem and incident management processes in place:

- Incident Management - Incident Management captures the details of all incidents reported, implements temporary work-arounds and manages the resolution of incidents. Its goal is to restore normal service operation with minimum disruption to the business.

- Problem Management - The goal of Problem Management is to minimize the adverse impact of incidents and “known errors” on the business. The main focus of Problem Management is to identify the root cause(s) of incidents and to eliminate these if this is possible. While problems are being resolved Problem Management may produce temporary ‘work-arounds.’

An incident is defined as an event which is not part of the standard operation of the T2S Service and which cause, or may cause, an interruption or a reduction of the quality of that service. Incidents must be resolved immediately and are not part of the Change and Release Management.

A problem is defined as an abnormal state or condition at the component, equipment, or sub-system level, which may lead to a failure in T2S that produces incorrect or unexpected results, showing a discrepancy between the relevant specifications and the actual results. Based on reported and acknowledged problems, and their criticality, T2S and the CSDs agree how to resolve them. A problem can result in a Change Request.

9.7 T2S SD.SUP 070: Service Level management services

T2S uses a Service Level Management process to maintain and improve service quality through a constant cycle of agreeing, monitoring and reporting of service achievements and instigating actions to correct non-adequate service delivery.

T2S provides reports on actual Service Levels achieved on a monthly basis. For each service indicator as defined in the Service Level Agreement, the performance achieved is compared with the target values. These reports are provided in accordance with the rules laid down in the Service Level Agreement.
9.8 T2S SD.SUP 080: Invoicing services

Invoicing services in T2S consist of:

- Automatically calculated invoices that are set up on a regular basis.
- On demand: Ad hoc invoicing in special cases (for CSDs / euro area or non-euro area NCBs and / or customers of CSDs / euro area or non-euro area NCBs).

For both types of invoices, i.e. T2S invoice to CSDs and CSD invoicing support, the invoice cannot be amended or adapted. Only

- approval;
- cancellation; and
- (re-) generation

are defined actions.

If a T2S Actor needs to receive a prior invoice (again), it can do so via a query in both A2A and in U2A mode.

9.8.1 T2S SD.SUP 081: T2S invoicing to CSDs and euro area or non-euro area NCBs service component

T2S automatically calculates invoices based on fees in accordance with the current T2S Tariff Structure and Price List. T2S invoicing reflects changes in the T2S Tariff Structure and Price List, which may be implemented at any time, but become effective only at the beginning of a billing period.

The invoice is calculated at the beginning of each calendar month for the past calendar month. All prices are calculated in Euro and VAT regimes in the different countries are taken into account, in case VAT needs to be included. Invoices and the underlying information are archived. CSDs and euro area or non-euro area NCBs receive a summary invoice, showing aggregate data for each billing item.

The prices for instructions are always charged to the CSDs of the two counterparties involved in a settlement instruction. Each Security Account and DCA needs to be assigned unambiguously to one CSD or euro area or non-euro area NCB for the billing of the fixed fees.

Invoices are sent out once via push mechanism to the technical address which is defined in the Common Static Data. The invoice can also be queried using the GUI. As an additional service, ad hoc billing is possible in special cases.
Changes in the Pricing scheme may be implemented at any time, but become effective only at the
beginning of the next billing period.

9.8.2 T2S SD.SUP 082: CSDs / euro area or non-euro area NCBs invoicing support service
component

T2S supports the CSDs/ euro area or non-euro area NCBs by enabling them to invoice their
clients in accordance with their individual tariff structures. To that end, as part of the T2S
information services, a CSD/ euro area or non-euro area NCB may query any of its assigned
accounts, but no others.

T2S provides counters for all settlement process steps and instances as enumerated and described
in the T2S data model. As part of the CSD/ euro area or non-euro area NCB invoicing support
service, each CSD/ euro area or non-euro area NCB is able to query this level of data for each of
its customer accounts.

T2S transmits details to the CSD/ euro area or non-euro area NCB via a report based on an event
at the end of the invoicing period. The CSD/ euro area or non-euro area NCB invoicing support
report provides additional information on billable items at the level of each customer account as
an itemised list. This is either sent in push mode or made available for pull mode.

Furthermore, on a monthly basis T2S provides a standard report containing all detailed
Transaction Data and counters for each CSD/ euro area or non-euro area NCB which is
available only to the respective CSD/ euro area or non-euro area NCB in pull mode. Each CSD /
euro area or non-euro area NCB receives only the data related to its and its DCPs interactions
with T2S, i.e. the invoicing support report is CSD- / euro area or non-euro area NCB - specific
and does not contain any data or information concerning any other CSD/ euro area or non-euro
area NCB.

9.9 T2S SD.SUP 090: Change and Release Management services

T2S is an evolving application, increasing and improving services by following a defined Change
and Release Management process. Any T2S Actor who identifies a need to change T2S, may
request new or amended features and/or functionalities following the agreed Change and Release
Management procedure, specified in Schedule 9 (Change and Release Management) to the
Framework Agreement and the Currency Participation Agreement. If there are inconsistencies
between the description in this section and the provisions of Schedule 9 (Change and Release
Management), the latter shall prevail.
1934 CSDs may change parameters/configuration (i.e. rules for CSD validation hold/reject and the
1935 CoSD functionality) or reference data (i.e. ISIN, Security Account) without launching the
1936 Change and Release Management, although these actions may be subject to operational
1937 procedures, in particular if there is an impact on any other T2S Actors.
1938 T2S uses ITIL based processes for Change and Release Management: These services encompass
1939 all stages of the Change Lifecycle from initiation and recording, through filtering, assessment,
1940 categorization, authorisation, scheduling, building, testing, implementation and ultimately their
1941 review and closure.
1942 The Eurosystem has established a Change Review Group (CRG) to evaluate the information
1943 provided in the Change Request and in the preliminary assessment (especially checking its
1944 consistency and completeness across all Change Requests) and to prepare for the change
1945 authorisation or rejection decision. The CRG is responsible for building and maintaining the
1946 scoring mechanism as a tool for facilitating the definition of the content of each T2S release and
1947 making proposals for, reviewing and monitoring the content of T2S releases as well as any
1948 changes to any agreed release.
1949 9.9.1 T2S SD.SUP 091: Change Management service component
1950 Changes in T2S, which are subject to the Change and Release Management, are defined as
1951 changes on T2S functionality and/or to the Scope Defining Set of Documents. Changes may arise
1952 for a number of reasons:
1953 ▪ innovation and improvement – the introduction of new services/ technical capability;
1954 ▪ new functionality to meet business needs of T2S Parties;
1955 ▪ changes in law or in regulatory (including fiscal) requirements; or
1956 ▪ clarifications/corrections to functional and/or technical documentation/gaps in line with
1957 the user requirements.
1958 T2S distinguishes between the following types of changes:
1959 - according to beneficiary:
1960 ▪ Common Changes include new features, functionalities or services which are
1961 implemented for the benefit of – and available without restrictions to – all T2S Actors.
1962 They have an impact on all T2S Actors and the costs are shared by all T2S Actors.
Specific Changes are any new feature, functionality or services which is not implemented as a Common Change, but which some CSDs/CBs wish to implement, and to which the other CSDs/CBs do not object. The costs of these changes are shared only by the entities using the feature, functionality or service, which is changed. The functionality is used only by the supporting parties but is made available to all T2S Actors.

- according to urgency:

- Normal changes are changes that can be planned and go through the whole Change and Release Management before being implemented into the live environment.

- Fast-track Changes are changes that are imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management or changes that are critical for the stability of the T2S Platform or by euro area or non-euro area NCB decisions related to safeguarding the currency/ies or related to crisis management measures to ensure financial stability and that, owing to the time constraints, have to be implemented in a shorter time frame than normal, which will be decided on an ad-hoc basis. These changes will also go through the normal CRM process, however, the length of the different process steps will be shortened on an ad-hoc basis, in particular for preliminary and detailed assessment.

Each change will be categorised based on the following parameters:

- Legal/Business importance
- Market implementation efforts
- Operational/technical impact
- Financial impact for T2S

Every initiated Change Request is identified via a Change Request identifier. All Change Requests are published and made available to all duly authorised T2S Actors in accordance with the agreed Governance arrangements and the agreed Change and Release Management procedure, specified in Schedule 9 (Change and Release Management) to the Framework Agreement and the Currency Participation Agreement.

In certain cases an incident may result in an urgent intervention on T2S aiming to ensure a quick restoration of T2S Services. On account of its urgency, such an intervention cannot be processed via the normal Change and Release Management. These Fast-track Changes are therefore processed via faster operational procedures as defined and further detailed in the Manual of Operational Procedures (MOP).
9.9.2 T2S SD.SUP 092: Release Management service component

Once the changes have been duly authorised for implementation, they are bundled and assigned to future T2S releases. The term “Release” is used to describe a collection of authorised Change Requests which consist of enhancements to the T2S Service and/or a number of bug fixes which are implemented into the production environment. A scoring mechanism is applied to identify all authorised changes and bug fixes for a specific release. The Release Management services include the planning, design, build, configuration and testing of T2S software and hardware needed for the implementation of the changes to create a set of release components.

The Release Management services ensure that all aspects of a change, technical and non-technical, are considered together. The main objective is to deliver, distribute and track one or more changes intended for simultaneous release into T2S operations while protecting the integrity of the T2S production environment and its services. Release Management services ensure that authorised changes and bug fixes that have been agreed as part of a release are secure and traceable, and that only correct, tested and authorised versions are installed into the production environment. Furthermore, through Release Management any amended legal or contractual obligations T2S has to comply with will be implemented.

Before implementing any release, T2S performs T2S-internal acceptance tests to verify that the system operates as predicted and fulfils the requirement and the functional specification of the Change Request.

Once T2S-internal acceptance test is finalised, T2S provides the CSDs and euro area or non-euro area NCBs with the test results and confirms the readiness of the T2S testing environments for the T2S User Testing. The test calendar is agreed with the CSDs and euro area or non-euro area NCBs, and information is provided on the testing activities, and regarding the availability of the testing environments.

The release is verified in accordance with the Governance arrangements, with the involvement of the CSDs and euro area or non-euro area NCBs once the exit criteria of the verification process have been completed successfully.

The delivery of the application software release into the production environment is the final step in the Release Management.

T2S provides and updates T2S Documentation as part of the Release Management.
9.10 T2S SD.SUP 100: Test and training services

9.10.1 T2S SD.SUP 101: Testing service component

The objectives of the T2S User Testing are:

- to ensure that T2S fully meets user requirements as expressed in the Change Requests of the relevant release, as well as the functional and non-functional specifications agreed by T2S; and
- to guarantee the readiness of the CSDs, euro area or non-euro area NCBs and its DCPs to operate in accordance with the agreed release.

T2S provides diverse testing environments for T2S Actor testing activities:

- one for the CSD/ euro area or non-euro area NCB wanting to test changes in their own applications against the current T2S operating environment; and
- other(s) for the CSD/ euro area or non-euro area NCB to test future T2S releases.

The T2S testing environments are sized and prepared for interconnection with the testing environments of the T2S Actors via test networks. T2S reserves the right to block one environment for its own regression testing of new releases.

The security levels of the testing environments are the same as for the T2S production environment. The testing environments have a substantially lower technical capacity compared to the production environment. This capacity can be increased to cover specific testing needs (e.g. high-volume tests during the Community testing and the Business Day testing stages). During the T2S User Testing execution phase, the T2S operating procedures reflect as much as possible those that are agreed for live operations.

T2S testing environments use the same problem and incident processes as the operating environment.

9.10.2 T2S SD.SUP 102: Training service component

T2S delivers training services to the CSDs, euro area or non-euro area NCBs and DCPs based on the “train the trainer”-concept. The exhaustive and self-explanatory T2S training documentation shall facilitate in-house training at CSDs, euro area or non-euro area NCBs and at their participants. The scope of the T2S training sessions covers aspects of the day-to-day activities of technical, functional and operational nature as well as one-off activities for the testing of and migration to T2S.

T2S provide the CSDs and the euro area or the non-euro area NCBs with the T2S Training Framework, on the basis of which T2S defines and elaborates the T2S Training Packages.
Depending on the training delivery strategy and mode selected (inherent in the T2S Training Framework), T2S guides, delivers and provides support for the T2S training for the CSDs and for the euro area or for the non-euro area NCBs.

The T2S Training Framework is elaborated and rolled out so that a timely and efficient knowledge transfer to the end-users of T2S can be accomplished. The T2S Training Framework further clarifies and details all organisational and planning aspects related to the training.
FRAMEWORK AGREEMENT

SCHEDULE 6

T2S SERVICE LEVEL AGREEMENT
# Framework Agreement

## Schedule 6 – T2S Service Level Agreement

## Table of contents

1. **Introduction** .......................................................................................................................... 3
2. **Parties, commencement date and scope** .............................................................................. 4
   - 2.1 IDENTIFICATION OF THE PARTIES........................................................................... 4
   - 2.2 SCOPE............................................................................................................................ 4
   - 2.3 COMMENCEMENT DATE............................................................................................ 4
3. **Service responsibilities** ......................................................................................................... 5
   - 3.1 EUROSYSTEM’S RESPONSIBILITIES.................................................................... 5
   - 3.2 CONTRACTING CSD’S RESPONSIBILITIES............................................................... 7
   - 3.3 OPERATIONAL PROCEDURES............................................................................... 9
   - 3.4 TECHNICAL NEUTRALITY..................................................................................... 10
4. **Service Levels in the production environment** .................................................................... 11
   - 4.1 DEFINITIONS OF SERVICE LEVEL INDICATORS...................................................... 11
     - 4.1.1 Service availability .............................................................................................. 11
     - 4.1.1.1 Availability period .......................................................................................... 11
     - 4.1.1.2 Substantial delay ........................................................................................... 12
     - 4.1.1.3 Availability ...................................................................................................... 12
     - 4.1.1.4 System performance ...................................................................................... 13
     - 4.1.1.5 Business Validation Time ............................................................................ 13
     - 4.1.1.6 Matching time ............................................................................................... 14
     - 4.1.1.7 Real-time Settlement time ............................................................................ 14
     - 4.1.1.8 Static data processing time ........................................................................... 15
     - 4.1.2 Response Times ..................................................................................................... 15
       - 4.1.2.1 A2A query response time ............................................................................ 17
       - 4.1.2.2 A2A message response time ...................................................................... 17
       - 4.1.2.3 U2A response time ...................................................................................... 17
       - 4.1.2.4 Online storage period .................................................................................. 18
       - 4.1.2.5 Archiving period .......................................................................................... 18
       - 4.1.2.6 Archive retrieval response time .................................................................. 18
     - 4.1.3 Support Hours and Incident Response Times ............................................................. 18
       - 4.1.3.1 T2S Settlement Day .................................................................................... 19
       - 4.1.3.2 Support hours ............................................................................................... 19
       - 4.1.3.3 Incident response time ................................................................................. 19
       - 4.1.3.4 Incident resolution time ............................................................................... 20
     - 4.1.4 Business Continuity and Disaster Recovery ................................................................ 20
       - 4.1.4.1 Recovery time ............................................................................................... 21
       - 4.1.4.2 Recovery point objective ............................................................................. 22
       - 4.1.4.3 Punctuality ..................................................................................................... 22
   - 4.2 COMMITTED SERVICE LEVELS FOR THE PRODUCTION ENVIRONMENT .................. 23
     - 4.2.1 Operational and Support Services ...................................................................... 23
     - 4.2.2 Settlement Services and Liquidity Management Services .................................... 25
     - 4.2.3 Static Data Services ............................................................................................ 26
     - 4.2.4 Information Services .......................................................................................... 26
     - 4.2.5 Connectivity Services ........................................................................................ 27
   - 4.3 TARGETED SERVICE LEVELS FOR THE PRODUCTION ENVIRONMENT .................... 27
     - 4.3.1 Settlement Services and Liquidity Management Services .................................... 27
     - 4.3.2 Static Data Services ............................................................................................ 27
     - 4.3.3 Information Services .......................................................................................... 27
     - 4.3.4 Connectivity Services ........................................................................................ 28
5. **Service Levels for the Test Environments** ......................................................................... 29
   - 5.1 SERVICE LEVELS FOR THE PRE-PRODUCTION ENVIRONMENT ............................... 29
     - 5.1.1 Operational and Support Services ...................................................................... 29
   - 5.2 SERVICE LEVELS FOR THE INTEROPERABILITY TEST ENVIRONMENT ....................... 30
     - 5.2.1 Operational and Support Services ...................................................................... 30
     - 5.2.2 Availability .......................................................................................................... 31
### Framework Agreement

#### Schedule 6 – T2S Service Level Agreement

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>5.3 ADDITIONAL PROVISIONS</td>
<td>31</td>
</tr>
<tr>
<td>57</td>
<td>6 System Capacity and Platform Sizing</td>
<td>33</td>
</tr>
<tr>
<td>58</td>
<td>7 Service Level Reporting</td>
<td>35</td>
</tr>
<tr>
<td>59</td>
<td>7.1 CONTENT OF THE REPORTING</td>
<td>35</td>
</tr>
<tr>
<td>60</td>
<td>7.2 DEFINITION OF ADDITIONAL INDICATORS FOR REPORTING</td>
<td>36</td>
</tr>
<tr>
<td>61</td>
<td>7.2.1.1 File throughput</td>
<td>36</td>
</tr>
<tr>
<td>62</td>
<td>7.2.1.2 Batch Settlement throughput</td>
<td>36</td>
</tr>
<tr>
<td>63</td>
<td>7.3 T2S OPERATIONS REPORT</td>
<td>37</td>
</tr>
<tr>
<td>64</td>
<td>7.4 T2S OPERATIONAL RISK REPORT</td>
<td>37</td>
</tr>
<tr>
<td>65</td>
<td>8 Service review meetings</td>
<td>38</td>
</tr>
<tr>
<td>66</td>
<td>9 SLA reviews</td>
<td>39</td>
</tr>
<tr>
<td>67</td>
<td>9.1 INITIAL REVIEW</td>
<td>39</td>
</tr>
<tr>
<td>68</td>
<td>9.2 SUBSEQUENT REVIEW</td>
<td>39</td>
</tr>
<tr>
<td>69</td>
<td>Annex 1 - Management of non-functional changes</td>
<td>1</td>
</tr>
<tr>
<td>70</td>
<td>1. EMERGENCY CHANGES</td>
<td>1</td>
</tr>
<tr>
<td>71</td>
<td>2. OTHER CHANGES</td>
<td>1</td>
</tr>
</tbody>
</table>
1 Introduction

This Service Level Agreement (SLA) documents the commitments of the parties named below to each other, in particular the Service Levels under which the Eurosystem will provide the T2S Services to the Participating CSDs that have entered into the Framework Agreement with the Eurosystem. The main objective of this document is to describe the Service Levels agreed between the parties and to define the Key Performance Indicators (KPIs) used to measure these Service Levels.

Annex 1 (Management of non-functional changes) to this document covers the process to manage non-functional changes needed to maintain the agreed Service Levels, or to increase them as a result of the SLA review process.

This SLA assigns responsibilities to and describes interactions between the parties. This SLA does not constitute liability other than specified in the provisions laid down in the Framework Agreement.

This SLA is part of the legal arrangements between the Eurosystem and CSDs, under the Framework Agreement. Unless explicitly mentioned this SLA is the same as the one concluded with all other CSDs. It is the intention of both parties to reach the highest possible level of harmonisation between all SLAs. The commitments of the Eurosystem and the CSDs set out below will not be altered without mutual agreement, subject to the agreed over-arching governance of T2S.
2 Parties, commencement date and scope

2.1 Identification of the Parties

The Parties to this Service Level Agreement are those indicated in the core Framework Agreement, i.e. the Eurosystem and the Contracting CSD.

As a matter of fact, the Directly Connected Parties (DCPs) do not have a direct legal relationship with the Eurosystem for the use of T2S Services. Nevertheless, they will obtain certain rights and be subject to certain obligations from this SLA through the mandatory inclusion of certain provisions in their legal arrangements with their CSD(s). These provisions are explicitly reflected in section 3.2 of this SLA.

2.2 Scope

This SLA relates to the production phase of T2S, as well as to the User Testing phase prior to a CSD’s migration to T2S. Consequently, this SLA refers to the T2S Production environment and its accompanying test environments both before and after migration. It covers the full range of services as described in Schedule 5 for each of the service classes, i.e. Settlement Services, Liquidity Management Services, Static Data Management Services, Information Services, Connectivity Services, and Operational and Support Services. In addition, this SLA covers the relevant service commitments from the Eurosystem with respect to the support of the User Testing activities as specified in Schedule 3 (User Testing).

2.3 Commencement date

This SLA shall enter into force as from the day the Contracting CSD starts its User Testing activities on the T2S Platform. More specifically, as from that day until the Contracting CSD migrates, the provisions with respect to the T2S test environments as specified in chapter 5 will apply. After the migration, these provisions shall apply again from the day any new release is made available in this environment until the go-live date of this new release.

In addition, as from the start of the first T2S Settlement Day, the Eurosystem is committed to deliver the T2S Services according to the Key Performance Indicators (KPIs) as specified in sections 4.2 of this SLA.
3 Service responsibilities

3.1 Eurosystem’s responsibilities

The Eurosystem must:

a) establish the T2S service desk as a single point of contact for the Contracting CSD (for technical and operational problems) and provide their contact details (e-mail, mobile phone, telephone, fax);

b) support the Contracting CSD in their operational management of direct links for the CSD and DCPs if needed;

c) ensure the permanent reachability of a T2S Crisis manager, T2S Operator’s Crisis manager, Service manager and T2S co-ordinator and provide their contact details (e-mail, telephone, fax);

d) refrain from scheduling system downtimes without pre-advice and green light of the Contracting CSD outside the normal Maintenance Windows;

e) announce planned non-functional changes according to the provisions specified in Annex 1 to this Schedule;

f) provide on-line access to information to allow the Contracting CSD to track and follow up all incidents, problems and enquiries related to or impacting the Contracting CSD;

g) provide a monthly Service Level Report to the Contracting CSD according to the provisions in section 7 of this SLA;

h) manage the impact on the Contracting CSD and the T2S Service as a whole caused by any T2S Actor making unusual demands on capacity by:

   a. contacting the service user without delay if the latter misbehaves, misuses T2S or consumes system resources in any other way to an extent that exceeds the forecasted capacity and might prevent the Eurosystem from delivering the agreed service to other service users;

   b. denying (up to and including temporary disconnection) providing the service to a service user if he is threatening the stability of the platform impacting other service users and does not respond effectively to the Eurosystem’s request to prevent further misbehaviour;

   i) deny the service by disconnecting any service user that did not respond effectively to a request from the Eurosystem to prevent a recurrence of previous misbehaviour and that
continues to threaten the stability of the platform with impact on other service users, until the service user has demonstrated that the threat no longer exists;
j) provide to the Contracting CSD historical data on the previous four quarters on the parameters laid down in section 6 of this SLA in order to facilitate the Contracting CSD's forecasting of business data for the next four quarters. The historical data will include the historical data of its DCPs;
k) The Eurosystem shall translate the Contracting CSD's forecasts into metrics that are relevant for estimating the T2S system capacity (ceiling);
l) ensure an adequate long-term planning for capacities corresponding to the requirements laid down in section 6 of this SLA;
m) inform the Contracting CSD if technical problems with one of its Directly Connected Parties (DCPs) are detected.
n) Maintain documentation pertaining to Crisis management and provide it to the Contracting CSD on request or after any change;
o) Support the Contracting CSD in business continuity testing if required (subject to prior agreement).

During normal operation, the T2S co-ordinator (appointed by the Eurosystem), the T2S Service manager (appointed by the T2S Operator) and the CSD settlement manager, will apply the procedures specified in the Manual of Operational Procedures (see also section 3.3). In addition, the Eurosystem stands ready to provide through the T2S service desk
 information on technical and operational issues, in particular the running of T2S;
 information on T2S functionality;
 up-to-date information concerning the running of T2S, if need be.

If a Crisis Situation, as described in Article 23 of the Framework Agreement, arises within the domain of the Eurosystem, the latter will inform the Contracting CSD according to the agreed response times.

In addition, the following provisions will apply in such case:
 The Eurosystem will take all necessary actions to restore the T2S Service according to the agreed business continuity procedures. These procedures are based on the following key principles:
  o Any settlement in T2S before the incident will continue to have the legal effect specified in Article 21.4 of the core Framework Agreement.
  o If a data loss materialised, the recovery will be done together with the Contracting CSD by procedural means.
As soon as the Eurosystem identifies the need switch to the other site in the same region, or to fail-over to the standby region, the T2S co-ordinator initiates a teleconference to inform the settlement manager of the Contracting CSD about the nature of the event triggering the failure, the nature of the failure and the envisaged plan to recover from the failure.

The Eurosystem will keep the settlement manager of the Contracting CSD informed about the progress of the failover activities, and in particular when T2S is available again for normal operations.

The Eurosystem may decide to gradually re-open T2S, in which case it will seek the approval of the Contracting CSD.

In case T2S cannot be restarted without a potential data gap, the Eurosystem will first re-open T2S for the purpose of reconciliation only, and will co-ordinate these reconciliation activities.

During this reconciliation phase, the Contracting CSD is responsible to verify the status of its T2S records, and to re-send instructions with the aim to bring the T2S records consistent with its internal records. This includes also changes to the T2S records that happened as a result of an interaction with a DCP belonging to the Contracting CSD. It is up to the Contracting CSD to agree with its DCPs how this is organised.

The Eurosystem and the Contracting CSD will co-operate in good faith and will - if necessary - agree on additional measures with the aim to close the data gap.

The Eurosystem will seek the agreement of the Crisis managers of the Contracting CSD and the Participating CSDs to re-open T2S for normal operations.

The Eurosystem will provide any service described for normal operations, but balancing this with the need to restore the service.

Throughout the whole Crisis management process, the Eurosystem will appropriately involve the DCPs, in accordance with the arrangements agreed with the Contracting CSD and Participating CSDs.

Detailed procedures for incident priority setting and incident handling will be specified in the Manual of Operational Procedures (MOP).

### 3.2 Contracting CSD’s responsibilities

In order to allow the Eurosystem to meet the agreed Service Levels, the Contracting CSD must:

- appoint and ensure the permanent reachability of a CSD settlement manager and a CSD Crisis manager as contacts for the Eurosystem and provide their contact details (e-mail, telephone, mobile phone, fax);
b) provide contact details for technical staff that is capable of resolving technical issues with their Directly Connected Parties (DCPs);

c) have a local service desk acting as a single point of contact for all its users during normal business hours;

d) proactively report any problem or incident relating to T2S including connectivity problems, provide all information that might be helpful and cooperate where requested by taking all appropriate actions for solving the problem or incident;

e) report such problems or incidents to the T2S service desk within a reasonable time;

f) provide timely information on any changes that may affect the provision of the services;

g) ensure an appropriate use of T2S and that the personnel who works on its systems and equipments is accordingly qualified and suitably trained;

h) ensure availability of skilled staff within a pre-agreed time period in order for the Eurosystem to obtain support in handling incidents and/or reducing their impact on the service;

i) provide on a quarterly basis updated forecasts for average business figures as specified in the URD, to allow the Eurosystem to make an adequate long-term capacity planning (see section 6 of this SLA). The Contracting CSD shall produce forecasts, in good faith, on a best effort basis, on the basis of (i) historical data provided by the Eurosystem, and (ii) information available to CSDs about their future business (at the moment of providing the forecast);

j) be able to resend – at the request of the Eurosystem - all messages already sent after a specified recovery point during the same Settlement Day (approx. two minutes - in particular in case of disaster recovery scenarios with possible data loss);

k) keep all access rights it has registered for access in T2S consistent with the duties and responsibilities of its employees;

l) ensure with the support of the Eurosystem that all its Directly Connected Parties (DCPs) receive, accept and understand all information to facilitate their smooth functioning in T2S;

m) ensure the operational management of its own organisation as well as their customers including DCPs;

n) ensure the operational management of the technical links to T2S from the CSD and DCPs with the support of the Eurosystem if needed;

o) take part in the test process for new releases in the test environment;
p) co-operate with the Eurosystem by promptly reporting any difficulties however small following each release into the production environment;

q) support the Eurosystem in business continuity testing if required.

3.3 Operational Procedures

The Manual of Operational Procedures (MOP) will provide a reference guide for the operational procedures (in normal and abnormal situations) which the Directly Connected T2S Actors (including the Contracting CSD) and the Eurosystem should follow to ensure a smooth functioning of T2S. It will contain all the information required for the addressees to carry out all their tasks in normal and abnormal situations.

The day-to-day operational management of T2S will be handled at two levels. First, the T2S co-ordinator, the service manager and the CSD settlement managers (jointly called the settlement managers) will jointly perform the tasks and apply the procedures as specified in the MOP. Second, the T2S Crisis manager, the T2S Operator’s Crisis manager and the CSD Crisis managers (jointly called “the Crisis managers”) will make the decisions allocated to them in the MOP, and will take over the management of T2S in situations that are not covered in the MOP. The Crisis managers will be assisted and advised by the settlement managers in that case.

The latter include the Business Continuity and Disaster Recovery arrangements, i.e. the set of rules and procedures aimed at resuming the normal T2S Services after the occurrence of an incident, as well as at mitigating the impact of such incident.

The key principles for the incident management can be summarised as follows:

If the Contracting CSD detects an incident that is related to or might have an impact on the T2S Services, it will inform the Eurosystem without undue delay.

If the Eurosystem detects an incident, it will be communicated to the Contracting CSD, if a direct or indirect impact is possible.

If an incident is reported by a DCP of the Contracting CSD, the Eurosystem will inform the latter without undue delay, and keep the Contracting CSD informed about the resolution path of such incident. Any action to escalate such incident, will be undertaken in close co-operation with the Contracting CSD.

Both sides will co-operate to reduce the impact of an incident.

As far as the incident management procedures defined in the MOP allow to handle a particular incident, the T2S co-ordinator (appointed by the Eurosystem), the T2S service manager (appointed by the T2S Operator) and the involved CSD settlement managers (appointed by each CSD) will co-operate in good faith, and exchange all relevant information that is necessary to handle the incident as specified in the MOP.
When the incident cannot be handled within the procedures specified in the MOP, the T2S Crisis manager (appointed by the Eurosystem), the T2S Operator’s Crisis manager, and the CSD Crisis managers (appointed by each CSD) will decide – in accordance with the applicable governance arrangements – which measures will be taken to mitigate the impact of the incident and to resume normal operations.

Both sides will co-operate in analysing the root-cause for an incident.

The Eurosystem will report on the results of the root-cause analysis. An initial report with the impact analysis will be provided within two Settlement Days. An interim report will be provided within one week and a final report within two weeks.

Whether or not a request to change a cut-off time, either from the Eurosystem or from the Contracting CSD, is related to an incident, the Eurosystem will involve the CSD Settlement managers and/or the CSD Crisis managers in making such decision, according to the procedures further specified in the MOP.

3.4 Technical neutrality

As a matter of principle, the Eurosystem shall make reasonable efforts to ensure that, in normal circumstances, no Directly Connected T2S Actor receives a different Service Level based on historic or forecasted volumes, its name, its country of legal incorporation or of the location of its data centres, or any other factor. Abnormal circumstances might require a temporary deviation from this principle.
4  Service Levels in the production environment

This section describes the Key Performance Indicators (KPIs) agreed for the delivery of the service during **normal operations** (arrangements for Crisis Situations see under “IT Service Continuity”). As a general principle, the Eurosystem has to ensure that sufficient efforts are made to fulfil all KPIs, and must take remedial action as soon as it detects that a KPI may not be, or is not, fulfilled.

The Contracting CSD is committed to provide all reasonable support to the Eurosystem, in order to allow the latter to take such action.

T2S is a service shared between several service users. All specified Service Levels are therefore multilateral service levels, i.e. they define the service provided to the community of service users as a whole. Nevertheless, the service level reporting will contain the achieved bilateral service levels for the Contracting CSD in addition to the achieved multilateral service levels. For this bilateral reporting, the Service Levels reported for the Contracting CSD will include the Service Levels obtained by its DCPs.

### 4.1 Definitions of Service Level Indicators

This chapter provides a common definition of the service level indicators. Section 4.1.1 covers availability, and 4.1.1.4 and 4.1.2 list the areas identified as requiring Service Level indicators covering system performance. 4.1.3 and 4.1.4 cover support and recovery issues. The actual agreed levels are stated for each service individually in section 4.2 below.

#### 4.1.1 Service availability

**Objective:**

These indicators define the times during which the T2S Services are available in relation to the T2S Settlement Days.

#### 4.1.1.1 Availability period

The availability period is the time period during the T2S Settlement Day when the service is stated as expected to be available to the Contracting CSD. The start and end time of the availability period is based on business events on the T2S Platform. Any times stated are indicative and could be altered in certain circumstances according to the Procedures specified in the Manual of Operational Procedures (e.g. delay of the end-of-day).
### 4.1.1.2 Substantial delay

If an event defined in the T2S daily schedule is likely to be implemented later than the scheduled and has a potential impact on the Contracting CSD, the substantial delay will define for each event the maximum delay that will be tolerated by the Contracting CSD. Any delay or expected delay exceeding the substantial delay will be communicated to the Contracting CSD’s service desk immediately.

Any delay not exceeding the substantial delay is not actively communicated to the Contracting CSD’s service desk, but is available for querying on the T2S Platform.

### 4.1.1.3 Availability

**Definition:**

A service is considered to be available when it responds and operates according to its definition in the T2S Service Description and its functional description in the User Detailed Functional Specification (UDFS chapter 1).

**Measurement:**

The availability of the services is measured continuously and objectively at pre-defined components of T2S, throughout each Settlement Day with the exclusion of the Maintenance Window.

The measurement of downtime is based on auditable data collected either automatically or manually. Manual measurements will be used in situations where no automatic log entries are available (e.g. power failure).

Downtime is the time between the start of an incident that causes the unavailability of a service and the closing of the incident that caused the downtime, i.e. when the service has been restored.

In case of multiple incidents at the same time the downtime begins with the start of the first incident and ends with the closing of the last incident.

**Calculation:**

\[
\begin{align*}
    a_i &= \left(1 - \frac{d_i}{T_m}\right) \times 100 \\
    a &= \sum_{i=1}^{n} a_i \times w_i
\end{align*}
\]

Where:

- \(a_i\) = availability of the service \(i\) as percentage
The availability of a service is expressed as a percentage of the aggregated downtime in relation to the aggregated expected up-time during the reporting period. The calculation is based on minutes.

The weights of the service (wi) used in the KPI calculations will be documented in the T2S Manual of Operational Procedures (T2S MOP), as amended from time

4.1.1.4 System performance

Objective:
These indicators define the system performance the Contracting CSD is expecting from the T2S Platform. T2S will be sized as a single shared environment on the basis of data supplied by service users (see section 6), with a margin for exceptional peaks (see 4.2.2). If the volumes processed in production exceed the estimated T2S system capacity, i.e. ceiling (see chapter 6), service performance commitments are not binding for the Eurosystem. In such scenario the operational day shall not be affected, the T2S platform shall function without incident and without the potential need of actions from the Contracting CSDs. In case the volumes exceed also the margin envisaged for the exceptional peaks (see 4.2.2), the service performance commitments are also not binding. In such scenario service performance breaches may occur and incident management procedures will be followed with the potential need of actions from the Contracting CSD to resolve the incident.

4.1.1.5 Business Validation Time

Definition:
The Business Validation Time is the time that elapses between the reception of an instruction by T2S and the end of the business validation process, i.e. the time when T2S triggers the generation of the acceptance or rejection message.

Measurement:
The Business Validation Time is measured based on timestamps created by the T2S network interface and the timestamps stored as part of the audit trail in the T2S database. The instructions
that are checked either against restriction types configurations with more than 10 market-specific attributes or a restriction type rule with more than 5 market-specific attributes, as well the instructions with linked instructions above 50 are excluded from the calculation.

4.1.1.6 Matching time

Definition:
The Matching time is the time that elapses between the end of a successful business validation and the end of the first Matching attempt. The end of a Matching attempt is marked by the time T2S triggers the generation of the Matching status notification message or the detection that there is not yet a Matching instruction available.

Measurement:
The Matching time is measured based on timestamps stored as part of the audit trail in the T2S database. If at the end of the matching process, there is a pool of more than 100 instructions meeting the mandatory matching criteria, excluding the settlement amount, those instructions are excluded from the calculation. This KPI does not apply during the 30 minutes following either the end of the weekly Maintenance Window¹ or the end of a daily Maintenance Window after a T2S closing day.

4.1.1.7 Real-time Settlement time

Definition:
The Real-time Settlement time is the period between the end of the creation of the matching object (i.e. after successful matching) and the end of the first settlement attempt. The end of the settlement attempt is marked by the time T2S triggers the generation of the settlement status notification message.

This indicator is relevant only for settlement instructions sent on the Intended Settlement Date after the start of the Real-time Settlement phase of T2S.

Measurement:
The Real-time Settlement time is measured based on timestamps stored as part of the audit trail in the T2S database.

Additional remarks:

¹ Please see Schedule 1 – Definitions.
For the T2S settlement process several cut-off times have been defined. The T2S Platform will ensure that each settlement instruction that has been sent and acknowledged before the relevant cut-off time will get at least one settlement attempt.

### 4.1.1.8 Static data processing time

**Definition:**

The static data processing time is the time that elapses between the end of a successful business validation and the end of the processing of this request.

This indicator is relevant only for all types of static data maintenance instructions.

**Measurement:**

The static data processing time is measured based on timestamps stored as part of the audit trail in the T2S database.

**Additional remarks:**

In Batch Settlement mode certain types of static data maintenance requests might be queued to ensure the consistency of the settlement processing. In these cases the processing is considered complete after the creation of a new revision for the relevant entities even though this revision is only activated at a later point in time.

### 4.1.2 Response Times

**Objective:**

Time indicators provided in the following sections are always measured within the T2S perimeter under the responsibility of the Eurosystem as shown by the dashed line in the diagram below. The actual transmission time of the data via the network between T2S and the Contracting CSD is not included in the response time.
The response time indicators define the time period between the reception of a request and the corresponding response of the T2S Platform. All performance indicators are measured during each T2S Settlement Day during the time window when the information services are expected to be available.
Additional remarks:

All messages that have been queued during the Maintenance Window and queries that have been queued during Batch Settlement will not be included in the calculation of the response times.

Simple queries and complex queries are those referenced as such within the User Detailed Functional Specifications (UDFS).

4.1.2.1 A2A query response time

Definition:

For A2A query requests the response time is defined as the time elapsed between the reception of the query request message and the completion of the sending out of the corresponding result message (see diagram above).

Measurement:

The response times for A2A queries are measured using the timestamps generated by the T2S network interface.

4.1.2.2 A2A message response time

Definition:

For all A2A requests other than A2A queries the response time is defined as the time elapsed between the reception of the request message by T2S and the sending out of the corresponding acknowledgement message (see diagram above).

This KPI does not apply for request messages sent within files.

Measurement:

The response times for A2A requests are measured using the timestamps generated by the T2S network interface.

4.1.2.3 U2A response time

Definition:

For all U2A requests the response time is defined as the time needed by the system to generate a web (HTML) page (i.e. the time it takes the server to generate the page, plus the time it takes the proxy to download the content from the server).

Measurement:

For U2A requests the response time is measured by the T2S Platform within the Eurosystem’s domain. In order to limit the effect of queries with a large number of business objects retrieved...
the response time is computed assuming that the duration of each U2A request is equal to the monthly average response time of that kind of web page.

4.1.2.4 Online storage period

The online storage period defines the minimum time T2S keeps Transactional and Static Data available online. For Transactional Data entities this period starts when the entity reaches its final status (i.e. settled, cancelled, etc.). For Static Data entities this period starts when the entity is no longer active and no longer referenced from a Transactional Data entity.

4.1.2.5 Archiving period

The archiving period defines the minimum time T2S keeps Transactional and Static Data available in an archive for retrieval by the Contracting CSD. For Transactional Data entities this period starts when the entity reaches its final status (i.e. settled, cancelled, etc.). For Static Data entities this period starts when the entity is no longer active and no longer referenced from a Transactional Data entity.

4.1.2.6 Archive retrieval response time

Definition: The archive retrieval response time is defined as the time elapsed between the reception of an archive retrieval request and the sending out of the corresponding notification that the data is available for download.

Measurement: The archive retrieval response time is measured using the timestamps generated by the T2S network interface.

4.1.3 Support Hours and Incident Response Times

Objective: These indicators define the response times of the T2S service desk in relation to the type of incident/request and the T2S Settlement Days. An incident is defined as any event which is not part of the standard operation of a service and which causes or may cause an interruption or a reduction in the quality of that service.

Incidents will be categorised in the following priority classes, irrespective of whether they are reported by the Contracting CSD, or by one of its DCPs:
Framework Agreement

Schedule 6 – T2S Service Level Agreement

<table>
<thead>
<tr>
<th>Incident Priority</th>
<th>Severity</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Priority 1        | Critical | Complete unavailability of all T2S Services  
|                   |          | Complete unavailability of one or more services for which no workaround is available. |
| Priority 2        | Urgent   | Unavailability of a service, but a workaround is available |
| Priority 3        | Medium priority | All services are available, but some are experiencing performance problems |
| Priority 4        | Low priority | Query or service request |

4.1.3.1 T2S Settlement Day

Definition:

A T2S Settlement Day is a day on which all T2S Services are planned to be running.

4.1.3.2 Support hours

Definition:

The T2S service desk can be contacted via telephone or e-mail by the Contracting CSD. During standard support hours the T2S service desk can be contacted to communicate technical or business problems on the Contracting CSD’s side, open tickets for failures of T2S and receive support by the T2S Operators. During non-standard support hours the T2S service desk should be initially contacted via telephone to communicate information that is urgently needed or useful to avoid or limit any negative impact on daily operations, as e-mails will not be monitored during this time. Any e-mail request that is sent during this time will be processed during the next standard support hours only unless it is pre announced by a telephone call and related to an ongoing priority classes:1 or priority 2 incident started outside standard support hours (see above).

4.1.3.3 Incident response time

Definition:

The incident response time is defined as the time between the incident being detected or information about the incident received by the Eurosystem and the start of the action to resolve the incident.

Measurement:
Upon acceptance of an incident or service request the T2S service desk will assign a reference number and a priority level (see section 4.1.3) to it. The reference number will allow the Contracting CSD to monitor the incident’s status in the trouble management information tool. Measurement is done based on the times recorded in the trouble management system.

**4.1.3.4 Incident resolution time**

**Definition:**

The incident resolution time of an incident is the time between the start of action to resolve the incident and the time it is actually solved or a workaround is available.

**Measurement:**

Upon acceptance of an incident or service request the T2S service desk will assign a reference number and a priority level to it. The reference number will allow the Contracting CSD to monitor the incident’s status in the online trouble management information tool. Unless the Contracting CSD formally objects promptly, both times above are the times recorded by the T2S service desk in the trouble management system.

**4.1.4 Business Continuity and Disaster Recovery**

**Objective:**

The Business Continuity and Disaster Recovery mechanisms for T2S are designed to manage failures that require on-site recovery, alternate site recovery and alternate region recovery to ensure a high availability of the T2S Platform.

Business Continuity and Disaster Recovery scenarios will be categorised in the following classes:
Class Description

Minor failure Minor failure is understood as a short service interruption (e.g. due to component failures, a system reboot, or a line failure). These problems may typically be solved at the primary site.

Major failure Major failure or disaster is understood as a serious service interruption (e.g. disruptions caused by fire, flood, terrorist attack or major hardware/telecommunications faults). These events require the activation of the service in an alternative site.

Regional disaster Regional disaster is understood as a "wide-scale regional disruption" causing severe permanent interruption of transportation, telecommunication, power or other critical infrastructure components across a metropolitan or geographical area and its adjacent communities; or resulting in a wide-scale evacuation or inaccessibility of the population within the normal commuting range of the disruption's origin.

These events require the activation of the service in an alternative region.

4.1.4.1 Recovery time

Definition:

The recovery time (RTO = recovery time objective) is defined as the maximum acceptable time to restart the T2S Platform after a failure.

Measurement:

The recovery time is measured as the time between detection of an incident that causes the unavailability of the T2S Platform as a whole (or significant parts of it) and the time the incident is resolved or a workaround is in place.

Where the agreed procedures foresee a consultation or decision of service users, the time between informing service users and the service users’ response is excluded from the recovery time, as is the time needed for reconciliation of lost data (see incident handling in chapter 3.1).

For the avoidance of doubt, activating the service in an alternative site (major failure) will preserve the status of instructions and transactions, both settled and non-settled. Within the constraints set by the recovery point objective (RPO) (see 4.1.4.2 below), this also applies to the re-activation of the service in an alternative region (regional disaster).
4.1.4.2 Recovery point objective

**Definition:**

The recovery point objective (RPO = recovery point objective) is defined as the maximum acceptable time interval for which data sent to and by T2S is lost when a restart takes place.

**Measurement:**

The recovery point is a point of consistency to which a user wants to recover or restart. The RPO is measured as the amount of time between the moment when the point of consistency was created or captured and that when the failure occurred.

4.1.4.3 Punctuality

**Definition:**

The punctuality of T2S is measured by counting the number of occasions when:

- the start of selected T2S business events are delayed for a time period exceeding the defined substantial delay (4.1.1.2);
- the duration of defined periods of the business day exceed agreed values.

**Measurement:**

The delays for the start of the event will be checked using the planned and the actual start time stamps for the relevant events as logged by T2S.

The following events are relevant for this calculation:

- Intraday Delivery versus Payment (DVP)\(^2\) cut-offs (one event per currency)
- Intraday Free of Payment (FOP)\(^3\) cut-off (IFOP)
- Change of the business day completed (BDCD)
- Start of Cycle 1 / Preparation of Sequence 0 (C1P0)

The following periods of the Business Day are relevant for the calculation of the KPI on the duration:

- Start of Day: from the start of the event BDCD to the end of the event End of Start of Day (ESOD)
- Night Time Settlement: from the start of C1P0 until the end of the NTS reporting (timestamps of the last message/file sent).
- Duration of IDVP: from the start till the end of the event IDVP.

\(^2\) Please see Framework Agreement, Schedule 1 – Definitions.
\(^3\) Please see Framework Agreement, Schedule 1 – Definitions.
### 4.2 Committed Service Levels for the Production Environment

#### 4.2.1 Operational and Support Services

<table>
<thead>
<tr>
<th>Response Times</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Storage Period (4.1.2.4)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>90 days</td>
</tr>
<tr>
<td>Archiving Period (4.1.2.5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10 years</td>
</tr>
<tr>
<td>Archive Retrieval Response Time (4.1.2.6)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>72 hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T2S Settlement Day (4.1.3.1)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all calendar days except: Saturdays, Sundays, days where all the T2S settlement currencies are closed</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Weighted Availability parameters (4.1.1.3)</th>
<th>Service</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A2A Connectivity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>U2A Connectivity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lifecycle Management and Matching</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Settlement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Liquidity Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Static Data Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Statistics, Queries, Reports, Archive</td>
<td>As defined in the T2S Manual of Operational Procedures (T2S MOP)</td>
</tr>
<tr>
<td></td>
<td>Operational Services</td>
<td></td>
</tr>
</tbody>
</table>
### Weighted Availability value

(4.1.1.3)  
\[ \geq 99.7\% \text{ / calendar month} \]

### Support Hours and Incident Response Times

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Standard Support Hours**  
(4.1.3.2) | from 6:30 am to 8:00 pm CET on all T2S Settlement Days except: Catholic/Protestant Easter Friday, Catholic/Protestant Easter Monday, and 1 May |
| **Non-Standard Support Hours**  
(4.1.3.2) | All times on T2S Settlement Days which fall outside the Standard Support Hours |
| **Incident Response Time**  
(4.1.3.3) | 15 min. during standard support hours  
60 min. during non-standard support hours |

### Incident Resolution Time

(4.1.3.4)  
<table>
<thead>
<tr>
<th>Incident Priority</th>
<th>During standard support hours</th>
<th>Outside standard support hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 hours</td>
<td>3 hours</td>
</tr>
<tr>
<td>2</td>
<td>Before the start of the next Settlement Day (minimum 2 hours)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2 Settlement Days or as agreed</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5 Settlement Days or as agreed</td>
<td></td>
</tr>
</tbody>
</table>

### Business Continuity and Disaster Recovery

<table>
<thead>
<tr>
<th>Recovery Type</th>
<th>Time Requirement</th>
</tr>
</thead>
</table>
| Recovery Time: minor failure  
(4.1.4.1) | See Incident Response/Resolution Time |
| Recovery Point Objective: minor failure  
(4.1.4.2) | No data loss |
| Recovery Time: major failure  
(4.1.4.1) | < 60 minutes (from the decision to failover to the 2\textsuperscript{nd} site in the same region) |
| Recovery Point Objective: major failure  
(4.1.4.2) | No data loss |
| Recovery Time: regional disaster  
(4.1.4.1) | < 120 minutes (from the decision to failover to the other region) |
### Framework Agreement

#### Schedule 6 – T2S Service Level Agreement

<table>
<thead>
<tr>
<th>Recovery Point Objective: regional disaster (4.1.4.2)</th>
<th>&lt; 2 minutes data loss</th>
</tr>
</thead>
</table>

#### Maintenance Windows

<table>
<thead>
<tr>
<th>Start of weekly Maintenance Window</th>
<th>Saturday (or the calendar day following the last T2S Settlement Day in a week) 3:00 CET or after sending out the last report after the Batch Settlement (whatever comes later).</th>
</tr>
</thead>
<tbody>
<tr>
<td>End of weekly Maintenance Window$^d$</td>
<td>Monday (or the first T2S Settlement Day in a week) 5:00 CET at the latest</td>
</tr>
<tr>
<td>Start of daily Maintenance Window</td>
<td>3:00 CET</td>
</tr>
<tr>
<td>End of daily Maintenance Window</td>
<td>5:00 CET</td>
</tr>
</tbody>
</table>

#### Punctuality

<table>
<thead>
<tr>
<th>Substantial Delay (4.1.1.2)</th>
<th>10 minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration of the IDVP cut-off</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Duration of the Start of Day Phase</td>
<td>75 minutes</td>
</tr>
<tr>
<td>Duration of the Night time Settlement phase</td>
<td>210 minutes</td>
</tr>
<tr>
<td>Duration of the End of Day phase</td>
<td>45 minutes-</td>
</tr>
</tbody>
</table>

#### 4.2.2 Settlement Services and Liquidity Management Services

#### System Capacity

<table>
<thead>
<tr>
<th>Maximum Matching Time (4.1.1.6)</th>
<th>95% within 60 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>5% within 60 and 180 seconds</td>
</tr>
<tr>
<td>Maximum Real-time Settlement Time (4.1.1.7)</td>
<td>95% within 90 seconds</td>
</tr>
<tr>
<td></td>
<td>5% within 90 and 270 seconds</td>
</tr>
</tbody>
</table>

$^d$ The Eurosystem stands ready to occasionally shorten the weekly Maintenance Window based on specific needs of the Contracting CSD (e.g. migration, issuance in direct holding countries). The latter shall pre-announce such needs sufficiently in advance and shall agree the start and end time of the relevant Maintenance Window(s) with the Eurosystem.
# System performance

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Margin for exceptional peaks</td>
<td>20% of the T2S System Capacity (ceiling) for the Number of instructions received, the Daily number of static data updates and Number of Securities Accounts (see chapter 6)</td>
</tr>
<tr>
<td></td>
<td>30 A2A queries per second (max 20,000 per hour)</td>
</tr>
</tbody>
</table>

## 4.2.3 Static Data Services

### Availability

<table>
<thead>
<tr>
<th>Availability Period</th>
<th>outside the Maintenance Windows on all T2S Settlement Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4.1.1.1)</td>
<td></td>
</tr>
<tr>
<td>Static Data Processing Time</td>
<td>95% within 20 seconds</td>
</tr>
<tr>
<td>(4.1.1.8)</td>
<td>5% within 20 and 120 seconds</td>
</tr>
</tbody>
</table>

## 4.2.4 Information Services

### Availability

<table>
<thead>
<tr>
<th>Availability Period</th>
<th>outside the Maintenance Windows on all T2S Settlement Days</th>
</tr>
</thead>
<tbody>
<tr>
<td>(4.1.1.1)</td>
<td></td>
</tr>
</tbody>
</table>

### Response Times

<table>
<thead>
<tr>
<th>Response Time</th>
<th>95% within 20 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2A Message Response Time</td>
<td>5% within 20 and 120 seconds</td>
</tr>
<tr>
<td>(4.1.2.2)</td>
<td></td>
</tr>
<tr>
<td>U2A Response Time</td>
<td>95% within 10 seconds</td>
</tr>
<tr>
<td>(4.1.2.3)</td>
<td>5% within 10 and 60 seconds</td>
</tr>
<tr>
<td>A2A Query Response Time for Simple Queries&lt;sup&gt;5&lt;/sup&gt;</td>
<td>95% within 20 seconds</td>
</tr>
<tr>
<td>(4.1.2.1)</td>
<td>5% within 20 and 120 seconds</td>
</tr>
</tbody>
</table>

---

Framework Agreement
Schedule 6 – T2S Service Level Agreement

| A2A Query Response Time for Complex Queries (4.1.2.1) | 95% within 5 minutes
| 5% within 5 and 15 minutes |

603 4.2.5 Connectivity Services

<table>
<thead>
<tr>
<th>System Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Business Validation Time (4.1.1.5)</td>
</tr>
<tr>
<td>95% within 60 seconds</td>
</tr>
<tr>
<td>5% within 60 and 180 seconds</td>
</tr>
</tbody>
</table>

604 4.3 Targeted Service Levels for the Production Environment

605 The more demanding, but non-binding target KPIs defined in this chapter reflect the Service Level, that is targeted by the Eurosystem. Even if these KPIs are not reached, but the Service Level is still within the range of the committed service levels (see chapter 4.2), this is no breach of the T2S Service Level Agreement. However, in such a case the Eurosystem stands ready to jointly investigate ways to improve the service.

610 4.3.1 Settlement Services and Liquidity Management Services

<table>
<thead>
<tr>
<th>System Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Matching Time (4.1.1.6)</td>
</tr>
<tr>
<td>99% within 60 seconds</td>
</tr>
<tr>
<td>1% within 60 and 180 seconds</td>
</tr>
<tr>
<td>Maximum Real-time Settlement Time (4.1.1.7)</td>
</tr>
<tr>
<td>99% within 90 seconds</td>
</tr>
<tr>
<td>1% within 90 and 270 seconds</td>
</tr>
</tbody>
</table>

611 4.3.2 Static Data Services

<table>
<thead>
<tr>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Data Processing Time (4.1.1.8)</td>
</tr>
<tr>
<td>99% within 20 seconds</td>
</tr>
<tr>
<td>1% within 20 and 120 seconds</td>
</tr>
</tbody>
</table>

612 4.3.3 Information Services

<table>
<thead>
<tr>
<th>Response Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2A Message Response Time (4.1.2.2)</td>
</tr>
<tr>
<td>99% within 20 seconds</td>
</tr>
<tr>
<td>1% within 20 and 120 seconds</td>
</tr>
</tbody>
</table>
Framework Agreement
Schedule 6 – T2S Service Level Agreement

| U2A Response Time (4.1.2.3) | 99% within 10 seconds
|                         | 1% within 10 and 60 seconds |
| A2A Query Response Time for Simple Queries (4.1.2.1) | 99% within 20 seconds
|                         | 1% within 20 and 120 seconds |
| A2A Query Response Time for Complex Queries (4.1.2.1) | 99% within 5 minutes
|                         | 1% within 5 and 15 minutes |

4.3.4 Connectivity Services

<table>
<thead>
<tr>
<th>System Capacity</th>
</tr>
</thead>
</table>
| Maximum Business Validation Time (4.1.1.5) | 99% within 60 seconds
|                         | 1% within 60 and 180 seconds |
5 Service Levels for the Test Environments

The non-binding target KPIs defined in this chapter reflect the Service Level, that is targeted by the Eurosystem for the test environments. Even if these KPIs are not reached there is no breach of the T2S Service Level Agreement. However, in such a case the Eurosystem stands ready to jointly investigate ways to improve the service.

5.1 Service Levels for the Pre-production environment⁶

5.1.1 Operational and Support Services

<table>
<thead>
<tr>
<th>Availability</th>
<th>From 7:00 to 19:00 CET on all calendar days except: Saturdays, Sundays, 1 January, Catholic/Protestant Easter Friday, Catholic/Protestant Easter Monday, 1 May, 25 December, 26 December or Days specified in the UTEST calendar managed by the OMG.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Support Hours and Incident Response Times</th>
<th>07:00 – 19:30 CET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Support Hours (4.1.3.2)</td>
<td>15 min. during standard support hours</td>
</tr>
<tr>
<td>Incident Resolution Time (4.1.3.4)</td>
<td>Incident Priority</td>
</tr>
<tr>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

⁶ Please see Framework Agreement, Schedule 3 – User Testing.
## Framework Agreement

### Schedule 6 – T2S Service Level Agreement

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>5 business days or as agreed</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>As agreed</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>As agreed</td>
</tr>
</tbody>
</table>

### Availability

- **Availability (4.1.1.3)**: 95% / calendar month
- **Availability Period (4.1.1.1)**: outside the Maintenance Window on all T2S Settlement Days

### Punctuality

- **Substantial Delay (4.1.1.2)**: 20 minutes
- **Duration of the IDVP cut-off**: 10 minutes
- **Duration of the Start of Day Phase**: 60 minutes
- **Duration of the Night time Settlement phase**: 90 minutes
- **Duration of the End of Day phase**: 45 minutes-

## 5.2 Service Levels for the Interoperability test environment

### 5.2.1 Operational and Support Services

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T2S Settlement Day (4.1.3.1)</td>
<td>From 7:00 to 19:00 CET on all calendar days except: Saturdays, Sundays, 1 January, Catholic/Protestant Easter Friday, Catholic/Protestant Easter Monday, 1 May, 25 December, 26 December and days specified in the Interoperability test environment calendar managed by the PMG.</td>
</tr>
</tbody>
</table>

---

7 Please see Framework Agreement, Schedule 3 – User Testing.
### Support Hours and Incident Response Times

<table>
<thead>
<tr>
<th>Incident Response Time (4.1.3.3)</th>
<th>Incident Priority</th>
<th>During standard support hours</th>
<th>Outside standard support hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>15 minutes</td>
<td>1 hour</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>15 minutes</td>
<td>Next business day</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1 day</td>
<td>Next business day</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1 day</td>
<td>Next business day</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Resolution Time (4.1.3.4)</th>
<th>Incident Priority</th>
<th>Incident Resolution Time</th>
<th>Status Call Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1-2 business days</td>
<td>2 hours</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2-5 business days</td>
<td>4 hours</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>According to agreed plan</td>
<td>Upon closure</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>According to agreed plan</td>
<td>Upon closure</td>
<td></td>
</tr>
</tbody>
</table>

### 5.2.2 Availability

#### Availability

<table>
<thead>
<tr>
<th>Availability (4.1.1.3)</th>
<th>85 % / calendar month</th>
</tr>
</thead>
</table>

#### Availability Period (4.1.1.1)

<table>
<thead>
<tr>
<th>Availability Period on all T2S Settlement Days</th>
</tr>
</thead>
</table>

### 5.3 Additional provisions

The test environment can be opened with extended hours for a limited period upon request.
The Eurosystem will make all reasonable efforts to ensure that the operational hours of the test environments, including on-line availability for end-users and batch processing capabilities for the end of day procedures will be specified in the T2S User Testing Calendar and might be different for each of the testing environments.

In certain cases such as the deployment of a new release, the Eurosystem reserves the right to change the T2S User Testing Calendar, which includes changing the opening and closing times of the test environments. All changes to the T2S User Testing Calendar shall be proposed, discussed and agreed in the substructure in charge of User Testing, before informing the T2S Users in a timely manner in advance.

The Information Security levels of the test environments shall be broadly the same as for the T2S production environment.

The test environments will have a substantially lower capacity compared to the production environment (10% of the long-term capacity model for the system capacity ceiling for the production environment).

The Eurosystem shall increase the capacity of the test environments to cover specific testing needs (e.g. high-volume tests during the community testing and the business day testing stages) upon a request from – and in agreement with – the Contracting CSD.

The T2S Service desk shall be the unique point of contact to report incidents and problems, and to ask for guidance on T2S during User Testing. The Contracting CSD can contact the T2S Service desk via phone, fax, and email.

The T2S Service desk coverage hours shall be aligned to the operation hours of the test environment referred to above.
## 6 System Capacity and Platform Sizing

To ensure the proper sizing of the T2S Platform that is required to meet the agreed Service Levels, the Eurosystem provides the Contracting CSD with historical data on a quarterly basis, for the previous four quarters, according to the indicators in the table below. The Contracting CSD is then requested to provide updated forecasts for the next four quarters for average business figures as specified below, to allow the Eurosystem to make an adequate long-term capacity planning. The figures of the historical data provided by the Eurosystem and of the forecasts provided by the Contracting CSD should include the volumes for the Contracting CSD’s DCPs as well. Forecasts are produced in good faith, on a best effort basis by the Contracting CSD, and translated by the Eurosystem into metrics that are relevant for estimating the T2S system capacity (ceiling). The SLA commitment is based on this estimation.

The following parameters are required for these calculations:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Number of instructions received</td>
<td>Quarterly average daily distribution of incoming instructions (in a breakdown for SoD, NTS, RTS and EoD). Historical data (average, minimum and maximum) for previous 4 quarters is provided by the Eurosystem and forecasts (average) are then provided by the Contracting CSD for the upcoming quarters.</td>
</tr>
<tr>
<td>2. Daily number of static data updates</td>
<td>The historical and expected number of insertions, modifications and deletions to be executed in T2S on one day. The historical data (average, minimum and maximum) for previous 4 quarters is provided by the Eurosystem and forecasts (average) are provided by the Contracting CSD.</td>
</tr>
<tr>
<td>3. Daily average of A2A queries</td>
<td>Previous 4 quarters’ minimum, maximum and average daily number of A2A queries is provided by the Eurosystem and forecasts (average) as foreseen for the next 4 quarters are provided by Contracting CSD.</td>
</tr>
<tr>
<td>4. Number of Securities Accounts</td>
<td>Total number of securities accounts (average, minimum and maximum) in the previous 4 quarters is provided by the Eurosystem and forecasts as foreseen for the next 4 quarters are provided by the Contracting CSD.</td>
</tr>
</tbody>
</table>

Abbreviations: SoD = Start of Day Phase; NTS = Night Time Settlement Phase; RTS = Real Time Settlement Phase; EoD = End of Day Phase.
In order to process exceptionally high peak volumes, the Eurosystem will ensure that additional processing capacity can be added on very short notice, provided no hardware components need to be replaced. However, there will be technical limitations to the extent of such a capacity increase. If the expectations change, the Contracting CSD will inform the Eurosystem. If exceptional capacity is needed for a one-time event or on shorter notice, the Eurosystem will try to cope with such requests, but on best effort basis only.
7 Service Level Reporting

End-to-end service reports including local service desk operations will be provided on a regular basis in electronic format, focusing on the above defined service metrics.

7.1 Content of the Reporting

In addition, these service reports will contain information on performance against the following indicators:

- resolution times of closed tickets
- escalation status of open tickets
- punctuality (see 4.1.4.3)

Performance against Service Level targets will be measured by the Eurosystem in compliance with the procedures agreed between the parties.

Reports on actual Service Levels achieved will be provided to the Contracting CSD on a monthly basis. This will cover for each service indicator the performance achieved compared with the target values. For informational purposes the Eurosystem will also report the bilateral service levels achieved for the Contracting CSD. These reports are to be provided to the Contracting CSD within ten Settlement Days after the end of each month.

On a daily basis and reflected in the monthly SLA report:

- Unresolved incidents
- Resolved incidents
- Actual service (including security) breaches
- Planned downtime
- Unplanned downtime

On a monthly basis:

- Service availability
- Frequency of incidents
- Cumulative service breaches
- Use of T2S service desk (when relevant)
- Application and technology performance specified in this document (i.e. input/output file throughput, statistics on incoming/outgoing messages)
- Planned changes
698  ▪  Previous month’s unresolved incidents
699  ▪  Previous month’s resolved incidents
700  ▪  Previous month’s unresolved problems
701  ▪  Previous month’s resolved problems
702  ▪  Comments and observations from the Eurosystem
703  ▪  Medium term trends of incident and their root cause analysis
704  ▪  Support figures (e.g. number of calls, response time, long abandon rate)
705  In addition to the technical indicators the monthly report will also contain other important
706  information like the following:
707  ▪  Updates to the T2S release calendar scheduling technical releases with an impact on the
708  Contracting CSD;
709  ▪  Information about upcoming changes without impact on the Contracting CSD;
710  ▪  Information about the planned implementation process (including the test strategy) and
711  timing for upcoming releases.

7.2 Definition of Additional Indicators for Reporting

712  This section defines additional indicators that are used for the reporting, but have no KPI attached
713  to it.
714  7.2.1 File throughput

716  Definition:
717  The file throughput is defined as the minimum number of megabytes per hour that the interface
718  subsystem has to be able to process in one hour independently for input and output.
719  Measurement:
720  The file throughput is measured by summing up the size of all files received during the reporting
721  period and dividing this value by the actual processing time needed. The processing time is
722  measured using the timestamps generated by the T2S network interface and as part of the T2S
723  audit trail

724  7.2.2 Batch Settlement throughput

725  Definition:
726  The Batch Settlement throughput is the ratio of the number of settlement instructions processed
727  and the time that elapsed for processing them (i.e. between the start and end of the processing
cycles). All instructions that are ready for settlement are considered regardless of whether they
have been settled or not.

Measurement:

The Batch Settlement throughput is measured based on timestamps stored as part of the audit trail
in the T2S database.

Calculation:

\[ R_n = \frac{I_n}{T_n} \]

Where:

\( R_n \) = Batch Settlement throughput
\( I_n \) = number of settlement instructions processed in Batch Settlement mode
\( T_n \) = cumulated Batch Settlement processing time

7.3 T2S Operations report

The Eurosystem will complement the Service Level report with the T2S Operations report. The aim of the report is to provide information on operational activities, settlement statistics and follow up of Service Level monitoring. The report is prepared on a monthly basis by the Eurosystem and shared with the Operations Managers Group and the T2S Steering Level.

7.4 T2S Operational risk report

The Eurosystem will complement the Service Level report with the T2S Operational risk report. The aim of the report is to provide information on operational risks and the monitoring the implementation of risk responses. The report is reviewed on a monthly basis by the Operations Managers Group and provided to the T2S Steering Level.
8 Service review meetings

The Eurosystem and the Contracting CSD will review the T2S service performance commitments during their regular meetings at Steering Level. In addition, the Eurosystem will convene on a monthly basis or upon request a meeting of the Operations Managers Group (OMG) to review the T2S service performance on a working level.

This meeting will evaluate the service performance since the last review. In particular the meeting will:

- Review the service achievement (service level target against actual performance)
- Review the Service Level Reports provided in recent periods. However, for the sake of intra-annual comparability, the Service Level Report format might be changed only on a yearly basis.
- Focus particularly on breaches of Service Levels
- Identify weak areas and potential ways to address problems and initiate service improvement
- Allow for a discussion on possible measures to improve settlement efficiency
- Preview issues (anticipated measures) for the coming period
9 SLA reviews

9.1 Initial review

All resulting changes to this SLA shall be approved by the parties. In case of persistent disagreement between the parties, the dispute resolution procedure laid down in the Framework Agreement shall be activated.

9.2 Subsequent review

The parties agree that the SLA will be reviewed on a yearly basis in order to verify the balance between evolving user requirements and defined T2S Service Levels, as well as to ensure the effectiveness of performance measuring criteria.

If required by the circumstances, the SLA can be reviewed on an ad-hoc basis.

Agreement review meetings provide an opportunity to review the agreement and associated targets. In particular the meeting will:

- Review service achievements with the customer and identifying potential improvement on both sides
- Review the service requirements and identify if any changes have occurred
- Discuss any changes that operations would like to make to the agreement
- Agree on the next step for the SLA: extension, changes or decommissioning.

Changes to the SLA will be agreed in accordance with the applicable governance arrangements specified in Schedule 8 (Governance) of the Framework Agreement, in particular through the involvement of the Operations Managers Group.
1. **Emergency Changes**

If an incident occurs, the Eurosystem may have to implement a change that cannot be delayed until the next planned Maintenance Window. The implementation of such a change will cause a system unavailability as described in section 4.2.1.

As a minimum, the Eurosystem will inform the Contracting CSD ex post about the reason for and the nature of the change. Nevertheless, the Eurosystem will make best efforts to inform the Contracting CSD ex ante, even at short notice.

2. **Other changes**

By default, changes aimed at ensuring that the Eurosystem is capable of delivering the T2S Services according to the KPIs specified in this SLA, or resulting from SLA reviews (see section 8), will be managed by the Eurosystem. If such changes have no impact on the Contracting CSD, the Eurosystem will inform the Contracting CSD ex ante about the nature and the date of such change.

If such changes have an impact on the Contracting CSD, or if the Contracting CSD expresses an interest in testing such changes, the Eurosystem and the Contracting CSD will co-operate in good faith to manage the changes, as much as possible and where relevant, following the provisions of Schedule 9 (Change and Release Management).

The dates reserved by the Eurosystem for implementing changes that have or might have an impact on the Contracting CSD, are documented in a calendar that is shared and agreed in advance with the Contracting CSD. Changes to this calendar will be reported in the monthly reporting as described in section 7. By default, changes are implemented during a Maintenance Window.

The Contracting CSD is responsible to involve its DCPs in the process if necessary and share the relevant information with them.
FRAMEWORK AGREEMENT

SCHEDULE 7

PRICING

1 January 2019
Table of contents

1 Introduction .............................................................................................................................. 1
2 T2S pricing policy ................................................................................................................... 2
3 T2S price list ............................................................................................................................ 3
4 T2S pricing structure ................................................................................................................ 4
   4.1 SUMMARY ....................................................................................................................................... 4
   4.2 SETTLEMENT SERVICES ................................................................................................................. 5
   4.3 INFORMATION SERVICES .............................................................................................................. 13
   4.4 TARIFF ITEMS INITIALLY PRICED AT ZERO ................................................................................ 16
   4.5 TARIFF ITEMS PRICED AT ZERO AT LEAST UNTIL END OF COST-RECOVERY PERIOD............... 19
5 Inventory of T2S service charges .......................................................................................... 20
   5.1 INTRODUCTION ............................................................................................................................. 20
   5.2 CHANGES ..................................................................................................................................... 20
      5.2.1 T2S Common Changes ............................................................................................................. 20
      5.2.2 T2S Specific Changes ............................................................................................................. 21
      5.2.3 Pricing of assessments of Change Requests ............................................................................. 21
   5.3 RTGS FEES FOR CONNECTING TO T2S .......................................................................................... 22
   5.4 TRAINING ...................................................................................................................................... 22
   5.5 CONSULTANCY .............................................................................................................................. 22
   5.6 REQUEST FOR AN ADDITIONAL TEST ENVIRONMENT ................................................................. 22
   5.7 SECURITIES REFERENCE DATA .................................................................................................. 23
   5.8 CONNECTIVITY SERVICES ............................................................................................................ 23
   5.9 ONE-OFF JOINING FEE .................................................................................................................. 23
   5.10 EXIT MANAGEMENT ...................................................................................................................... 23
   5.11 EXTERNAL EXAMINER .................................................................................................................. 23
   5.12 REIMBURSEMENTS OF COSTS FOR STORING DATA .................................................................. 23
1 Introduction

The Schedule on Pricing consists of four components: (i) the T2S Pricing policy, which describes the Governing Council decision on the Pricing of T2S Services (ii) the T2S price list, which gives the actual T2S prices in eurocent for each of the T2S Services (i.e. settlement, account management and information services); (iii) the T2S pricing structure, which provides a detailed description of the items in the T2S price list, as well as the related fee triggers; and (iv) the Inventory of T2S service charges, which provides a description of how T2S will finance changes to T2S, and a number of other services not covered in the T2S price list.

All prices are displayed on the T2S price list without VAT, which is not applied to T2S Services.

The procedures for the exercise, allocation and payment of claims under Articles 21, 28, 32, 33 and 40 of the Framework Agreement are detailed in Schedule 13 (Procedure for Payment of Claims).

Following the establishment of the T2S pricing policy in 2010, the Eurosystem revised the pricing levels in 2018, seeking broad market advice. It will continue to do so when discussing possible changes to the Pricing Schedule.
2 T2S pricing policy

The Governing Council of the European Central Bank (ECB) decided to set the Delivery versus Payment price for TARGET2-Securities (T2S) at 15 eurocent per instruction. This price was fixed for the period from the T2S Go-Live Date (22 June 2015) until December 2018.

The commitment to set the price at 15 eurocent was subject to the following conditions: (i) non-euro currencies add at least 20% to the euro settlement volume; (ii) the securities settlement volume in the EU is no more than 10% lower than the volumes projected by the T2S Programme Office, which are based on market advice; and (iii) tax authorities confirm that the Eurosystem will not be charged VAT for the T2S Services it provides.

In 2018, the Governing Council revised the pricing policy of T2S in the light of the start of operations in June 2015, and of the end of the migration period in September 2017. In doing so, it agreed new baselines for the T2S Pricing with the market representatives, to continue pursuing full cost recovery, whilst maintaining the pricing structure unchanged, in terms of the different weights for the tariff items.

The price list in Section 2 reflects the pricing level agreed within the updated baselines, consisting in a basis DvP of 19.5 eurocent with an additional 4-eurocent surcharge linked to the perspective volumes developments. The resulting figure of 23.5 eurocent remains the basis for the pricing structure.
## T2S price list

<table>
<thead>
<tr>
<th>Tariff items</th>
<th>Price (eurocent)</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settlement services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery versus Payment</td>
<td>23.5</td>
<td>per instruction†</td>
</tr>
<tr>
<td>Free of Payment</td>
<td>14.1</td>
<td>per instruction†</td>
</tr>
<tr>
<td>Payment Free of Delivery</td>
<td>14.1</td>
<td>per instruction†</td>
</tr>
<tr>
<td>Internal T2S liquidity transfer</td>
<td>14.1</td>
<td>per transfer</td>
</tr>
<tr>
<td>Account allocation</td>
<td>4.7</td>
<td>per instruction</td>
</tr>
<tr>
<td>Matching</td>
<td>4.7</td>
<td>per instruction</td>
</tr>
<tr>
<td>Intra-balance movement</td>
<td>9.4</td>
<td>per transaction</td>
</tr>
<tr>
<td><strong>Auto-collateralisation service with Payment Bank</strong></td>
<td>23.5</td>
<td>for issue and return, charged to collateral provider</td>
</tr>
<tr>
<td>Intended Settlement Date failed transaction</td>
<td>23.5</td>
<td>surcharge per Settlement Day failed per instruction†</td>
</tr>
<tr>
<td>Daytime settlement process</td>
<td>4.7</td>
<td>surcharge per instruction†</td>
</tr>
<tr>
<td><strong>Auto-collateralisation service with Central Bank</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instruction marked with 'top or high priority'</td>
<td>0*</td>
<td>surcharge per instruction†</td>
</tr>
<tr>
<td>Cancellation</td>
<td>0*</td>
<td>per instruction</td>
</tr>
<tr>
<td>Settlement modification</td>
<td>0*</td>
<td>per instruction</td>
</tr>
<tr>
<td><strong>Information services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A2A reports</td>
<td>0.4</td>
<td>Per business item in any A2A report generated</td>
</tr>
<tr>
<td>A2A queries</td>
<td>0.7</td>
<td>Per query business item in any A2A query generated</td>
</tr>
<tr>
<td>U2A queries</td>
<td>0.4</td>
<td>Per executed search function</td>
</tr>
<tr>
<td>Messages bundled into a file</td>
<td>0.4</td>
<td>Per message in a file</td>
</tr>
<tr>
<td>Transmissions</td>
<td>1.2</td>
<td>Per transmission</td>
</tr>
<tr>
<td><strong>Account management services</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Securities Account</td>
<td>Free of charge**</td>
<td>Fee options: a) monthly fee per ISIN in the account or</td>
</tr>
<tr>
<td>Fee per T2S Dedicated Cash Account</td>
<td>0***</td>
<td>b) monthly fee per account</td>
</tr>
</tbody>
</table>

† Two instructions per transaction are charged.

†† The auto-collateralisation with payment bank (i.e. client-collateralisation) is charged in line with the usage of T2S resources; only the collateral provider is charged. One collateralisation item plus both instructions of each auto-collateralisation leg are charged per ISIN and providing account, i.e. X cents * 5 (i.e. 1 collateralisation item + 4 settlement instruction) for each auto-collateralisation service with payment bank, where X is the price of settlement instructions and collateralisation items.

‡‡ T2S is sized in accordance with an expected consumption pattern, i.e. the anticipated distribution of settlement volumes during night-/day-time and peak hours. These items were initially set at a zero price, presuming that actual usage of T2S would remain within this expected consumption pattern over time. However, should there be a stronger than expected use of T2S resources and the volume distribution pattern be different than expected thus adversely affecting T2S performance, it will be reconsidered to charge for these items. The Eurosystem regularly reviews the actual volumes against expected patterns for the different items.

** Account management services for Securities Accounts are set at zero and will not be changed until the end of the cost recovery period, at least.

*** Account management services for T2S Dedicated Cash Accounts (DCAs) are not charged, presuming that the actual number and usage of DCAs will remain within expected consumption patterns. However, should DCAs involve a stronger than expected use of T2S resources thus adversely affecting T2S performance, it will be reconsidered to charge for these items. The Eurosystem regularly reviews the matter together with the Central Banks operating the DCAs.

1 January 2019
## T2S pricing structure

### 4.1 Summary

<table>
<thead>
<tr>
<th>Settlement services</th>
<th>DvP weight factor</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery versus Payment</td>
<td>100% per instruction</td>
<td></td>
</tr>
<tr>
<td>Free of Payment</td>
<td>60% per instruction</td>
<td></td>
</tr>
<tr>
<td>Payment Free of Delivery</td>
<td>60% per transfer</td>
<td></td>
</tr>
<tr>
<td>Internal T2S liquidity transfer</td>
<td>60% per transfer</td>
<td></td>
</tr>
<tr>
<td>Account allocation</td>
<td>20% per instruction</td>
<td></td>
</tr>
<tr>
<td>Matching</td>
<td>20% per instruction</td>
<td></td>
</tr>
<tr>
<td>Intra-position movement</td>
<td>40% per transaction</td>
<td></td>
</tr>
<tr>
<td>Intra-balance movement</td>
<td>40% per transaction</td>
<td></td>
</tr>
<tr>
<td>Auto-collateralisation service with Payment Bank</td>
<td>100% for issue and return, charged to collateral provider</td>
<td></td>
</tr>
<tr>
<td>Intended Settlement Date failed transaction</td>
<td>100% surcharge per Settlement Day failed per instruction</td>
<td></td>
</tr>
<tr>
<td>Daytime settlement process</td>
<td>20% surcharge per instruction</td>
<td></td>
</tr>
<tr>
<td>Daytime congestion charge</td>
<td>0% additional surcharge per instruction</td>
<td></td>
</tr>
<tr>
<td>Auto-collateralisation service with Central Bank</td>
<td>0% for issue and return, charged to the collateral provider</td>
<td></td>
</tr>
<tr>
<td>Instruction marked with 'top or high priority'</td>
<td>0% surcharge per instruction</td>
<td></td>
</tr>
<tr>
<td>Cancellation</td>
<td>0% per instruction</td>
<td></td>
</tr>
<tr>
<td>Settlement modification</td>
<td>0% per instruction</td>
<td></td>
</tr>
</tbody>
</table>

### Information services

- A2A reports: Per business item in any A2A report generated
- A2A queries: Per queried business item in any A2A query generated
- U2A queries: Per executed search function
- Messages bundled into a file: Per message in a file
- Transmissions: Per transmission

### Account management services

- Securities Account: Free of charge
- Fee per T2S Dedicated Cash Account: 0% Monthly

---

1 January 2019
4.2 Settlement services

The general principle is that each completed settlement service activity are counted and reflected in the relevant monthly bill. Unless indicated otherwise, billable events are charged based on the date in which T2S successfully executes the related instructions/the events occur.

Two counterparties to a settlement transaction initiate one instruction each and the two instructions are then matched and form one transaction.

The T2S Pricing structure aims at charging for resource usage in most instances. The price for settlement services is set relative to a DvP settlement.

Each partial settlement\(^1\) is charged separately (e.g. a settlement instruction settled in three parts is charged the DvP or FoP price three times, and any of the parts settled in the period 07:00 – 18:00 will attract the daytime surcharge).

Conditional securities delivery\(^2\) transactions are charged according to their individual components, e.g. DvP or FoP, matching, blocking and unblocking, creation of a condition and release of a condition, i.e. hold and release.

Section 4.4 contains the list of items which are initially set at a zero price, presuming that actual usage of T2S will be within the expected anticipated distribution of settlement volumes during night-/day-time and peak hours.

Section 4.5 contains the list of items which are priced at zero and will not be charged until the end of the cost recovery period, at least.

---

\(^1\) Partial settlement is defined in the URD as “a process that settles only a fraction of settlement instructions original volume and amount when full settlement is not possible due to lack of securities. The residual unsettled volume and amount may settle at a later stage during the Intended Settlement Date. Any residual amount at the end of the intended settlement date results in the reporting of a failed settlement”.

\(^2\) Conditional securities delivery is defined in the URD as “a procedure in which the final securities and/or cash booking is dependent on the successful completion of an additional action or event (e.g. registration of shares, cash settlement outside T2S)”.

---

1 January 2019
20 Delivery versus Payment

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 23.5 per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>100% (the numeraire)</td>
</tr>
<tr>
<td>Background</td>
<td>The DvP requests a simultaneous transfer of securities versus cash. Both instructing parties are charged. The DvP price constitutes the numeraire for other instruction related charges (i.e. other instruction charges are indicated as a percentage of the DvP price). Realignment instructions resulting from a DvP are not charged.</td>
</tr>
<tr>
<td>Fee trigger</td>
<td>Each successfully completed DvP settlement.</td>
</tr>
</tbody>
</table>

21 Free of Payment

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 14.1 per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>60%</td>
</tr>
<tr>
<td>Background</td>
<td>The FoP requests a transfer of securities only. There is no cash processing required. Both parties to the FoP are charged. Realignment instructions resulting from a FoP are not charged.</td>
</tr>
<tr>
<td>Fee trigger</td>
<td>Each successfully completed FoP settlement.</td>
</tr>
</tbody>
</table>

23 Payment Free of Delivery

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 14.1 per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>60%</td>
</tr>
<tr>
<td>Background</td>
<td>The PFOD requests a transfer of cash only. There is no securities processing required. Both parties to the PFOD are charged. Realignment instructions resulting from a PFOD are not charged.</td>
</tr>
<tr>
<td>Fee trigger</td>
<td>Each successfully completed PFOD settlement.</td>
</tr>
</tbody>
</table>
Internal T2S liquidity transfer

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 14.1 per transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>60%</td>
</tr>
</tbody>
</table>

**Background**

Internal liquidity transfers between two T2S Dedicated Cash Accounts are charged with a DvP weight factor of 60%.

Liquidity transfer charges are invoiced to T2S Users via the T2S Users’ Central Bank.

Payments triggered as part of a DvP are included within the DvP instruction charge.

**Fee trigger**

All successfully executed liquidity transfers between two T2S Dedicated Cash Accounts.

The fee is charged to the instructing party, i.e. the debited party.

Account allocation

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 4.7 per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>20%</td>
</tr>
</tbody>
</table>

**Background**

An account allocation in a “direct holding market” is an instruction involving at least one Securities Account which has been flagged as an “end-investor account” in T2S. Two instructions per transaction are charged. If the account allocation instructions are sent unmatched, the Matching fee is charged in addition. The definitions of a “direct holding market” and “end-investor account” in the context of the T2S Pricing Schedule are provided below.

*For the purpose of T2S Pricing, a “direct holding market” is defined as a market:*

1. in which, at a minimum, for holdings of domestic securities generally held by domestic residents, end-investors (retail investors in particular) would generally have an account directly in the Issuer CSD; and

2. which brings all segregated end-investor accounts to T2S that contain securities that are available in T2S.

For the purpose of T2S Pricing, the following markets are considered as
direct holding markets according to paragraph 1: Cyprus, Denmark, Estonia, Finland, Greece, Iceland, Malta, Norway, Romania, Slovakia, Slovenia, Sweden. This list is subject to review by the T2S Governance bodies when needed, following the procedure for ‘Decision-making on relevant matters other than Change Requests’ in Schedule 8 (Governance).

Definition of “end-investor accounts” and instructions eligible for the reduced account allocation fee

For the purpose of T2S Pricing, there are two options which a CSD serving a direct holding market in T2S can choose with respect to the definition of “end investor accounts and the instructions which are eligible for the account allocation fee:

Option A for a direct holding market in T2S:

a. All segregated accounts of customers of CSD participants are eligible to be flagged as ‘end-investor account eligible for the account allocation fee’. It is the responsibility of the respective CSD in a direct holding market in T2S in cooperation with its participants to ensure a proper flagging of accounts.

b. FoP instructions involving at least one account flagged as ‘end-investor account eligible for the account allocation fee’ are charged the account allocation fee, which is applicable to both sides of the FoP transaction.

Or:

Option B for a direct holding market in T2S:

a. All retail investor accounts are eligible to be flagged as ‘end-investor account eligible for the account allocation fee’. A retail investor means a ‘retail client’ in the meaning of MiFID II (OJ L 173 12.6.2014). It is the responsibility of the respective CSD in a direct holding market in T2S in cooperation with its participants to ensure a proper flagging of accounts.

b. DvP and FoP instructions involving at least one account flagged as ‘end-investor account eligible for the account allocation fee’
are charged the account allocation fee, which is applicable to both sides of the transaction.

The following principles apply to account allocations:

1. The objective of the fee for account allocations is to ensure a level playing field in T2S between direct and indirect holding markets.

2. As a principle, the account allocation fee should not be used for transactions in direct holding markets in T2S that would have been charged the full price in an average indirect holding market or in an average direct holding market opting for a layered model in T2S.

3. In line with the transparency principle of T2S, the T2S Board reports on an annual basis about the share of DvP transactions, FoP transactions and Account allocations in each of the respective direct holding markets in T2S. This report includes the share of DvP transactions and FoP transactions of the aggregated indirect holding markets in T2S for comparison.

Fee trigger: The fee trigger depends on which option A or B is chosen by the respective CSD serving a direct holding market in T2S:

- Option A. Any FoP instruction involving at least one account flagged as 'end-investor account eligible for the account allocation fee' is charged the account allocation fee, which is applicable to both sides of the FoP transaction.

Or:

- Option B. Any DvP or FoP instruction involving at least one account flagged as 'end-investor account eligible for the account allocation fee' is charged the account allocation fee, which is applicable to both sides of the transaction.

Matching

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 4.7 per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>20%</td>
</tr>
<tr>
<td>Background</td>
<td>An unmatched instruction will have to pass through the Matching process</td>
</tr>
</tbody>
</table>
and will assume additional processing resources of T2S. Therefore, it attracts a standard Matching charge on top of the regular settlement instruction fee. The Matching charge is 20% of a DvP instruction charge and is applied to both parties.

<table>
<thead>
<tr>
<th>Fee trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each successfully completed Matching event.</td>
</tr>
</tbody>
</table>

### Intra-position movements

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 9.4 per transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>40%</td>
</tr>
</tbody>
</table>

**Background**

All intra-position movements in the case of securities (i.e. blocking/ unblocking/ reservation/ unreservation/ earmarking / unearmarking) attract an instruction-based fee. Internally generated intra-position movements are also charged. For example, say a securities position is blocked for a specific DvP transaction. Once the DvP transaction which is using the blocked securities is ready to be settled, T2S will first have to unblock the securities position so the DvP can settle. This unblocking is charged. Examples are available in the UDFS. No fees are applied for the blocking of static data (i.e. of the Party, Securities Account). The intra-position movement fee are charged to respective T2S Users via their CSD.

<table>
<thead>
<tr>
<th>Fee trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any successfully executed intra-position movement.</td>
</tr>
</tbody>
</table>
### Intra-balance movements

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 9.4 per transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>40%</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td><em>All intra-balance movements in the case of cash (i.e. blocking/unblocking) attract an instruction-based fee. Internally generated intra-balance movements are also charged. The fees are also applied for the automatic release of cash blockings during end-of-day and the regenerated cash blockings at the next start-of-day in the case of a Conditional Securities Delivery (CoSD). No fees are applied for the blocking of static data (i.e. of the Party, Securities Account). The intra-balance (cash) movement fee are charged to respective T2S Users via their Central Bank.</em></td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td><em>Any successfully executed intra-balance movement.</em></td>
</tr>
</tbody>
</table>

### Auto collateralisation service with Payment Bank

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 23.5 per transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td><em>The complete auto-collateralisation with a Payment Bank attracts an all-in-one fee of 100% DvP weight factor for issue and return: one collateralisation item plus both instructions of each auto-collateralisation leg are charged per ISIN and providing account. Only the collateral provider is charged.</em></td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td><em>Each successfully executed auto-collateralisation transaction with a Payment Bank within the monthly billing period.</em></td>
</tr>
</tbody>
</table>

### Fail on Intended Settlement Date

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 23.5 per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Background</strong></td>
<td><em>Matched settlement instructions failing to settle on their Intended Settlement Date (ISD) are re-introduced into all the future settlement cycles until they either settle or are cancelled by the two counterparties. The daily charge addresses the resource cost of congestion and of the additional processes required to recycle a failed transaction, e.g. eligibility checking. Disciplinary</em></td>
</tr>
</tbody>
</table>
actions are not applied by T2S through its price list. Both parties of the failing settlement transaction will attract the charge.

| Fee trigger | Each Matched DvP, FoP, or PFOD which does not settle on its Intended Settlement Date attracts a surcharge. Furthermore, the surcharge is applied for every Settlement Day that the instruction fails to settle after the ISD. The charge is applied to both parties of the transaction. |

### Daytime settlement process

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 4.7 surcharge per instruction settled during the period 07:00 - 18:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>20%</td>
</tr>
<tr>
<td>Background</td>
<td>Settlement instructions successfully executed during the period 07:00 – 18:00 attract a 20% “daytime surcharge”.</td>
</tr>
<tr>
<td>Fee trigger</td>
<td>Any DvP, FoP or PFOD instruction successfully settled during the period 07:00 – 18:00 attract the daytime surcharge.</td>
</tr>
</tbody>
</table>
4.3 Information services

Reports, queries and messages of Directly Connected Parties (which are entitled to do so by the respective CSD) are charged to the CSD of the Directly Connected Party. Reports, queries and messages of a Payment Bank are charged to the Central Bank of the Payment Bank. Reports, queries and messages that are received/generated during peak hours, i.e. the last two hours prior to the DvP cut-off time (i.e. indicatively between 2 p.m. – 4 p.m.), may be subject to the daytime congestion surcharge.

For the purposes of the pricing of information services, the following definitions are used:

- A ‘business item’ is one instance of a business entity defined in the T2S data model (e.g. settlement instruction, securities position, intra-balance movement, liquidity transfer, cash posting, Securities Account, Dedicated Cash Account etc.) with all its attributes.

- A ‘message’ is an encrypted inbound/outbound communication used for Application-to-Application (A2A) interactions between T2S and its participants. A complete list of all messages is available in Chapter 3 of the User Detailed Functional Specifications (UDFS).

- A ‘file’ is a structured collection of ‘messages’.


### A2A reports

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 0.4 per business item in an A2A report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Background</strong></td>
<td>A2A reports are charged based on the reported number of business items. The list of A2A reports and associated business item is included in Annex 1 to Schedule 7.</td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td>Any A2A report generated, with the charge based on the reported number of business items.</td>
</tr>
</tbody>
</table>

### A2A queries

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 0.7 per queried business item in an A2A query</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Background</strong></td>
<td>A2A queries are charged based on the number of queried business items. The list of A2A queries and associated business item is available in Annex 1 to Schedule 7.</td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td>Any A2A query generated, with the charge based on the number of queried items.</td>
</tr>
</tbody>
</table>
## U2A queries

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 10 per executed U2A query</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Background</strong></td>
<td>U2A queries are submitted via the GUI and the U2A query response is received by the GUI. U2A queries viewed on the GUI are charged a fixed fee per executed query. If a U2A query were downloaded/exported, then it is charged in the same manner as for A2A queries (i.e. per business item in the downloaded U2A query). The list of U2A queries and associated business item is available in Annex 1 to Schedule 7.</td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td>Any executed U2A search function viewed on the GUI is charged a fixed fee. If a U2A query is downloaded, it is additionally charged in the same manner as for A2A queries (i.e. per queried business item).</td>
</tr>
</tbody>
</table>

### Messages bundled into a file

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 0.4 per message in each file containing bundled messages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Background</strong></td>
<td>T2S Actors have the possibility to send messages to T2S and receive messages from T2S bundled together into a file. Messages received by T2S which are not accepted or not successfully authenticated are not charged for.</td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td>Each file containing bundled messages, with the charge based on the number of messages in the file.</td>
</tr>
</tbody>
</table>

## Transmissions

<table>
<thead>
<tr>
<th>Price</th>
<th>Eurocent 1.2 per transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Background</strong></td>
<td>All types of transmissions (with the exception of technical acknowledgement messages) are counted and charged for.</td>
</tr>
<tr>
<td><strong>Fee trigger</strong></td>
<td>Each transmission per T2S Party (both inbound and outbound) is counted and charged for (except for technical acknowledgement messages).</td>
</tr>
</tbody>
</table>
Some worked examples for the pricing of information services:

<table>
<thead>
<tr>
<th>Item</th>
<th>Transmission fee (in eurocent)</th>
<th>Business item fee (in eurocent)</th>
<th>Fixed fee</th>
<th>Total charge</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2A report sent to a T2S Actor containing 100 business items</td>
<td>1.2 eurocent (for sending the report)</td>
<td>40 eurocent (100 x 0.4 eurocent for each business item contained in the report)</td>
<td>-</td>
<td>41.2 eurocent</td>
</tr>
<tr>
<td>A file containing 100 messages, sent by a T2S Actor to the T2S Platform</td>
<td>1.2 eurocent (for receiving the file)</td>
<td>40 eurocent (100 x 0.4 eurocent for each message bundled into the file)</td>
<td>-</td>
<td>41.2 eurocent</td>
</tr>
<tr>
<td>A2A query request and the subsequent response containing 100 business items</td>
<td>2.4 eurocent (1.2 eurocent for the A2A query request message and 1.2 eurocent for the A2A query response)</td>
<td>70 eurocent (100 x 0.7 eurocent for each queried business item)</td>
<td>-</td>
<td>72.4 eurocent</td>
</tr>
<tr>
<td>100 (individual) messages sent by T2S to a T2S Actor</td>
<td>120 eurocent (100 x 1.2 eurocent for each message)</td>
<td>-</td>
<td>-</td>
<td>120 eurocent</td>
</tr>
<tr>
<td>U2A query on the GUI</td>
<td>-</td>
<td>-</td>
<td>10 eurocent</td>
<td>10 eurocent</td>
</tr>
<tr>
<td>U2A query containing 100 business items, viewed on the GUI and then subsequently downloaded</td>
<td>-</td>
<td>70 eurocent (100 x 0.7 eurocent for each queried business item)</td>
<td>10 eurocent (for the initial viewing on the GUI)</td>
<td>80 eurocent</td>
</tr>
</tbody>
</table>
4.4 Tariff items initially priced at zero

T2S is sized in accordance with expected consumption patterns, i.e. the anticipated distribution of settlement volumes during night-/day-time and peak hours. The items in this section are set at a zero price, presuming that actual usage of T2S remains within the expected consumption patterns over time. However, should there be a stronger than expected use of T2S resources and the volume distribution pattern be different from expected thus adversely affecting T2S performance, these items may be charged. The Eurosystem regularly reviews the actual usage of T2S resources against expected consumption patterns.

Daytime congestion charge

<table>
<thead>
<tr>
<th>Price</th>
<th>Zero eurocent per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>0%</td>
</tr>
<tr>
<td>Background</td>
<td>An additional congestion surcharge may be applied to settlement instructions successfully executed during the last two hours prior to the DvP cut-off time (i.e. indicatively between 14:00 – 16:00). Initially this “congestion charge” is set at 0 eurocent but if it is found that too many instructions are executed during the period and hence causing congestion, a fee may be applied.</td>
</tr>
<tr>
<td>Fee trigger</td>
<td>Any DvP, FoP or PFOD instruction successfully settled during the last two hours prior to the DvP cut-off time (i.e. indicatively between 14:00 – 16:00) would attract the daytime congestion surcharge.</td>
</tr>
</tbody>
</table>

Auto collateralisation service with a Central Bank

<table>
<thead>
<tr>
<th>Price</th>
<th>Zero eurocent per transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>0%</td>
</tr>
<tr>
<td>Background</td>
<td>All transactions resulting from auto-collateralisation with a Central Bank would be charged an all-in-one fee. Only the collateral provider would be charged.</td>
</tr>
<tr>
<td>Fee trigger</td>
<td>All successfully processed auto-collateralisation transactions with a Central Bank within the monthly billing period.</td>
</tr>
</tbody>
</table>
### Daytime settlement of ‘high’ priority and ‘top’ priority instructions

<table>
<thead>
<tr>
<th>Price</th>
<th>Zero eurocent per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Background**

All ‘Top Priority’ and ‘High Priority’ instructions settled during the period 07:00 – 18:00 would be subject to a surcharge.

**TOP priority** = default assigned to instructions fulfilling predetermined criteria, such as those of trading platforms (multilateral trading facilities, Stock Exchanges, etc.) with and without a central clearing counterparty (CCP) as well as over the counter (OTC) instructions with a CCP (URD 7.2.2.2). Special instructions assigned by Central Banks or CSDs with a ‘reserved priority’ (e.g. Central Bank monetary policy operations) would attract the same charge.

**HIGH priority** = can be assigned by T2S Users to OTC transactions (without CCP) in the relevant settlement instruction. High priority instructions follow in the processing hierarchy after top priority instructions (URD 7.2.2.3).

**Fee trigger**

Instructions flagged with ‘Top Priority’ or ‘High Priority’ which are settled in the period 07:00 – 18:00. If a CSD’s priority traffic exceeds 20% of its total settlement volume within the monthly billing period, the Eurosystem discusses the matter with the respective CSD to assess the reason for such high usage. Should usage not be brought into a range below 20%, the CSD will be billed for the priority fee and charges may apply after a notification period of 60 days.

### Cancellation

<table>
<thead>
<tr>
<th>Price</th>
<th>Zero eurocent per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Background**

The cancellation of a settlement instruction which had been submitted previously needs to be validated and the original settlement instruction is flagged as successfully cancelled. In cases where the instruction has already been matched, each side of the cancellation would be charged.
<table>
<thead>
<tr>
<th>Fee trigger</th>
<th>instructions which are not successfully executed or have been denied are not charged.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>All instructions that have been successfully cancelled. Successful automatic cancellation of settlement instructions by the Instruction Maintenance Module would also be charged. All previously attracted chargeable status (e.g. Matched, partial settlement, Intended Settlement Date fail) would be charged as well.</td>
</tr>
</tbody>
</table>

### Settlement modification

<table>
<thead>
<tr>
<th>Price</th>
<th>Zero eurocent per instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>DvP weight factor</td>
<td>0%</td>
</tr>
</tbody>
</table>

**Background**

Settlement instruction modifications include any change of the Hold status (CSD hold status/ CSD validation hold status/ party hold status/ CoSD hold status), all release instructions, change of priority, change of partial settlement indicator and linkage block.

All relevant default settings do not attract a charge because they are driven by the relevant static data.

<table>
<thead>
<tr>
<th>Fee trigger</th>
<th>Any successfully executed settlement modification instruction leading to a change in status.</th>
</tr>
</thead>
</table>

### Fee per T2S Dedicated Cash Account

<table>
<thead>
<tr>
<th>Price</th>
<th>Zero euro monthly per T2S Dedicated Cash Account</th>
</tr>
</thead>
</table>

**Background**

Monthly fixed fee to cover for the maintenance of the static data.

This fee would be charged to respective T2S Users via their Central Bank.

| Fee trigger | Any T2S Dedicated Cash Account with the account status 'open' at the end of the monthly billing period or if it was closed during the billing period. |
### 4.5 Tariff items priced at zero at least until end of cost-recovery period

#### Securities Account fees

Securities Account fees are set at zero at least until the end of the cost recovery period.

<table>
<thead>
<tr>
<th>Price</th>
<th>Option a) Zero eurocent monthly per ISIN in a Securities Account</th>
<th>Option b) Zero euros monthly per Securities Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background</td>
<td>Increased numbers of ISINs in an account in general means more resource associated with maintaining static data for the account. T2S parties have the choice between:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Option a) each Securities Account open in the database of T2S and active during the billing period attracts a monthly fixed fee which is be applied for each ISIN held in the account; or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Option b) each Securities Account open in the database of T2S attracts a monthly fixed fee to cover for the maintenance of a Securities Account static data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Should CSDs offer the option, T2S Users can choose which option to be applied. The decision should be stable in the long term.</td>
<td></td>
</tr>
<tr>
<td>Fee trigger</td>
<td>Option a) All ISIN positions at the end of the monthly billing period within a Securities Account which was active during the billing period and the account flagged to be charged by ISIN attracts a fixed fee per ISIN position in the account</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Option b) Any Securities Account not flagged to be charged by ISIN with the account status ‘open’ at the end of the monthly billing period attracts a fixed fee. This fixed fee is also applied to accounts closed during the billing period.</td>
<td></td>
</tr>
</tbody>
</table>
5 Inventory of T2S service charges

5.1 Introduction

The Inventory of T2S service charges (the Inventory) provides T2S Users with a description of how T2S will finance changes (which, depending on the type of change, could potentially result in increases of T2S prices included in the T2S price list), and a number of other services not covered in the T2S price list. The present content of the Inventory is not necessarily exhaustive, but could potentially be expanded to encompass other types of service charges. If the list were to be expanded at a later stage, the general principle of charging at cost shall remain.

5.2 Changes

The process for how changes will be implemented to the T2S Services is described in Schedule 9 on ‘Change and Release Management’. The following section describes how the costs for Common Changes and Specific Changes of the T2S Services are to be recovered.

5.2.1 T2S Common Changes

Common Changes are defined as “any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is implemented for the benefit of all T2S Actors”. Prior to going ahead and implementing a Change Request, the Eurosystem will specify the development and running costs of the change. This will be a binding offer on behalf of the Eurosystem.

Those Common Changes that are classified as “corrective maintenance” (i.e. fixing of errors in coding, design or detailed specifications (bug fixes)) and “technical maintenance” (i.e. software adaptations and/or testing activities imposed by changes of the hardware or the operating system or other infrastructural software packages within certain resource limits) will not be charged separately.

All other Common Changes will first need to be financed by the Eurosystem and the Governing Council needs to decide to increase the financial envelope of T2S by the cost of such a change. Substantial increases in the financial envelope could result in the need to adjust the T2S price list at some stage and/or to lengthen the amortisation period and/or to establish separate amortisation cycles. The development costs, running costs and capital costs associated with these Common Changes will therefore have to be recovered through T2S fees (see T2S price list) over an amortisation period.

CSDs commit to bear any residual costs related to Common Changes requested by them that cannot be recovered through T2S fees.
5.2.2 T2S Specific Changes

Specific Changes are defined as “any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is not supported by all T2S Actors”. Based on the principle of non-exclusiveness and non-discrimination, the functionality would in principle be available to all initial and future T2S parties. However, those not wishing to use the new functionality would not be impacted and therefore would not bear any of the costs.

Prior to a Specific Change Request being approved, the Eurosystem will specify the full financial consequences associated with the change (e.g. the implementation costs, the running costs, capital costs and potentially lost revenues). The estimate of the implementation costs will be a binding offer on behalf of the Eurosystem.

Once the Specific Change Request has been approved and before the Eurosystem starts development activities, the entities requesting the change (“requesters”) will formally commit to bear the full financial consequences of the change and agree with the T2S Board on the financing of the Specific Change. The financing of Specific Changes may be in the form of either pre-financing, financing via transaction fees levied on the use of the specific functionality or any other recovery method to be agreed between the requesters and the T2S Board.

Entities which have not been part of the original agreement between the Eurosystem and the requesters to develop a specific functionality but decide to use such functionality at a later stage (“late-joiners”) will have to bear an appropriate share of the financial consequences. The requesters that initially requested the specific functionality shall seek an agreement with the late-joiner(s) for the revised allocation of financial consequences of such functionality. If original requesters and the late-joiner(s) cannot find an agreement on the revised allocation of the full financial consequences of that functionality, a panel of experts (nominated by CSDs in line with Arbitration rules) will decide on a revised allocation, using objective criteria in order to ensure non-discrimination, to avoid duplication of Specific Changes and to keep T2S open for new developments. Subject to the late-joiner having paid or committed to pay its share of the full financial consequences of the Specific Change in accordance with the revised allocation, it will be able to use the specific functionality.

5.2.3 Pricing of assessments of Change Requests

Preliminary assessments of a request for a functional change will attract a charge of €2,000. If, based on the results of the preliminary assessment, the party then decides to request a detailed assessment for the functional change, the detailed assessment will attract an additional charge of €10,000.

If the Change Request is subsequently approved and implemented, either as a Common Change or Specific Change, the costs of the preliminary and detailed assessments will be added to the total cost of the change (and recovered in the manner described in sections 5.2.1 and 5.2.2).
If the change is rejected, the costs of the preliminary and detailed assessment would be charged directly to the requester. In case there is more than one requester, the costs of the preliminary assessments and detailed assessments would be distributed equally.

5.3 RTGS fees for connecting to T2S

If an RTGS system charges T2S a fee for connecting to T2S, T2S will not charge this fee to its Contracting CSDs. T2S will annually charge such fee back to the Central Bank that operates the T2S Dedicated Cash Account in the currency in which the RTGS system operates. As a matter of service, T2S will annually provide each Central Bank operating a T2S Dedicated Cash Account with each Payment Bank’s annual share in the total number of postings on that T2S Dedicated Cash Account and the Central Bank might take that into account when allocating the charges.

5.4 Training

The Eurosystem will provide training by qualified trainers to interested parties on the structural and operational aspects of T2S. Such general training which T2S offers to all T2S Stakeholders will be free of charge. Tailor-made training will be charged to the requesting party on a per diem basis. The Eurosystem will charge training services at cost. T2S training course offerings and associated charges will be published on a regular basis.

5.5 Consultancy

The Eurosystem may provide resources on request of a CSD, Central Bank or a Directly Connected Party to provide advice and support improving their technical infrastructure interaction with the T2S platform. Specific consultancy will be charged to the requesting party on a per diem basis. The Eurosystem will charge the consultancy services that it provides at cost.

5.6 Request for an additional test environment

The Eurosystem will be providing two test environments for User Testing during migration and post-migration without charging any additional service charge. The Eurosystem will provide additional test environments subject to an approved Change Request. If CSDs/Central Bank would require additional test environments, the set-up costs of the test environment as well as daily maintenance fees will be charged at cost either as a Common or a Specific Change. If the additional test environment(s) is charged as a Specific Change, the fee will be included in the respective CSD/Central Bank bill as soon as the relevant test environment is ready for testing.
5.7 Securities Reference Data

If the Eurosystem were to provide the securities maintaining services to CSDs, it will charge these services at cost.

5.8 Connectivity Services

[The Eurosystem allows all CSDs and NCBs, and their customers, i.e. Directly Connected Parties and Dedicated Cash Account holders respectively, to connect to T2S via a Value Added Network.]

5.9 One-off joining fee

A CSD joining T2S will pay a one-off joining fee in the amount of 25% of the annual fee that this CSD will pay to T2S, calculated on the basis of the fee paid in the first full year of T2S operation of the CSD in question. The fee will be calculated and charged one year after the CSD will have started its operations in T2S.

5.10 Exit Management

If a CSD terminates the T2S Framework Agreement for convenience, the Eurosystem will invoice the CSD at cost for all planning, co-ordination and execution of exit activities that go beyond normal operational support. This will also be the case if a CSD decides to exit because the relevant non-euro area NCB no longer outsources its currency. If a CSD has terminated the Framework Agreement for cause, the Eurosystem will provide the support for exit activities free of charge.

5.11 External Examiner

In case of a regular or special examination, as provided in Article 26.4 and 26.6 of T2S Framework Agreement, 50% of the total cost charged by the External Examiner shall be borne by the Eurosystem and 50% by the CSD(s).

5.12 Reimbursements of costs for storing data

If a CSD requests the Eurosystem to maintain documentation and records for a period longer than specified in Article 26.9 of the T2S Framework Agreement, the Eurosystem is entitled to reimbursement of any reasonable costs incurred as a result of such further maintenance.
FRAMEWORK AGREEMENT

SCHEDULE 8

GOVERNANCE
Table of contents

Preamble ............................................................................................................................. 1

1 The decision-making process ...................................................................................... 3

1.1 Governance bodies ................................................................................................. 3

1.2 Decision-making on Change Requests ..................................................................... 4

1.3 Decision-making on relevant matters other than Change Requests ...................... 5

2 Additional Governance arrangements ....................................................................... 7

2.1 Prioritisation .............................................................................................................. 7

2.2 Changes driven by Legal and Regulatory Requirements ......................................... 8

2.3 Transparency ............................................................................................................ 9

2.4 Technical groups supporting the Governance bodies .............................................. 9

Annex - Mandate of the CSG ......................................................................................... 1

21 February 2018
Preamble

This Schedule sets out the Governance, i.e. the set of rules and procedures concerning the management of T2S Services, including the related procedures for decision-making and the roles of T2S Stakeholders therein. The Governance applies as of the Agreement Date and shall govern the Development Phase and the Operational Phase of TARGET2-Securities (T2S).

The parties agree that:

1. The aim of the Governance principles is to provide each T2S Stakeholder with the level of control necessary in further pursuing its commercial and policy objectives and to seek compliance with Legal and Regulatory Requirements. However, the parties agree that, since T2S is a multilateral environment, their level of control is necessarily lower than if each T2S signatory had its own environment.

2. Control is necessary to ensure that T2S operates safely and efficiently. Moreover, control shall allow change to be achieved and managed so as to ensure that changes that are proposed by one party/parties can be introduced without unduly affecting the other party/parties.

3. In order to achieve the necessary balance of control, it is very important that transparency is ensured and that all T2S Stakeholders are closely involved in the Governance of T2S. It is essential to ensure that T2S meets the evolving needs of the market in a consensual way. Transparency shall assure the T2S Stakeholders that final decisions will not be taken before their positions are considered by the relevant Governance body and by the other T2S Stakeholders. For this reason, technical and policy documents, such as the User Requirements Document, the Economic Impact Analysis and the T2S Governance arrangement were extensively discussed with market participants and published on the T2S’s website. The Eurosystem intends to continue doing so.

4. The procedure for the decision-making on Change Requests ensures, on the one hand, that CSDs keep the main responsibility for the evolution of the rules concerning the core of their settlement activity as they outsource to T2S a core part of their IT functions (the processing of Transfer Orders and the technical maintenance of their Securities Account database). In doing so, they need to comply with Legal and Regulatory Requirements and be able to exercise a sufficient degree of control over the functioning rules of Securities Accounts. The procedure also ensures, on the other...
hand, that the Governing Council will not have to implement measures that are not compliant with the mandate of central banks in general, with the statute of the European System of Central Banks and of the ECB in particular, or that would conflict with the interest of the smooth functioning of T2S.

5 The use of a single multilateral infrastructure by the Contracting CSD and Participating CSDs inevitably affects the way in which the Contracting CSD and Participating CSDs exercise their management and control functions in respect of the operations outsourced to T2S. At the same time, the Eurosystem provides harmonised T2S Services, thereby fulfilling its statutory tasks. This constitutes an outsourcing relationship different from a conventional one since it requires that the outsourcing service be constructed not exclusively by reference to the specific needs of the outsourcer (i.e. the CSDs) but also according to the public tasks entrusted to the outsourcee (i.e. Eurosystem).

6 Users, i.e. the customers of CSDs, and ultimately issuers and investors are the eventual beneficiaries of T2S. Their demands have to be appropriately taken into account when further developing T2S functionalities in order to ensure that T2S continues to meet the needs of the market.

On the basis of the above considerations, Section 1 explains the relationship of the different Governance bodies in the decision-making process. Additional Governance arrangements are outlined in Section 2.
1 The decision-making process

1.1 Governance bodies

The following T2S Governance bodies are involved in the decision-making process in accordance with Article 27 of the Framework Agreement:

Figure 1: T2S Governance bodies

Note: * The T2S Board is the Eurosystem Governance body at the Steering Level for matters which have been delegated by the Governing Council. The T2S Board liaises with other Eurosystem internal governance structures for issues of common concern.

** The ECB routes the reporting and the information to the respective addressees.
1.2 Decision-making on Change Requests

1. Any individual Participating CSD, the Contracting CSD, User member in the AG, euro area NCB, non-euro area NCB, the ECB or the 4CB may initiate a Change Request.

2. The Change Request is prepared by the Change Review Group (CRG) according to the procedures described in Schedule 9 (Change and Release Management). The CRG submits its deliverables to the CSD Steering Group (CSG) via the ECB. The ECB also provides the CRG deliverables to the T2S Board, the Non-euro Currencies Steering Group (NECSG) and the T2S Advisory Group (AG) and publishes the deliverables on the T2S website. Should any of the before-mentioned Governance bodies fail to provide its view within a reasonable amount of time, taking into account the urgency of the Change Request, this Governance body is then assumed to have agreed with the Change Request and the decision-making procedure continues.

3. If the Change Request was related to safeguarding the integrity of the respective currency and/or financial stability as part of crisis management measures, transparency could be limited to the contracting T2S Actors (the Contracting CSD, Participating CSDs and Central Banks) upon request of a Central Bank. Such Change Requests shall be made transparent at the latest when the change is taken up in a release.

4. The AG gives its advice on the Change Request within a reasonable amount of time, taking into account the urgency of the Change Request. The advice of the AG is addressed to the T2S Board and it shall be published on the T2S’s website.

5. The CSG takes a resolution on the Change Request within a reasonable amount of time, taking into account the urgency of the Change Request. The resolution of the CSG is addressed to the T2S Board and it shall be published on the T2S website.

6. The NECSG takes a resolution within a reasonable amount of time, taking into account the urgency of the Change Request. The resolution of the NECSG is addressed to the T2S Board and it shall be published on the T2S’s website.

7. A final decision on the Change Request is taken by the Governing Council on the basis of a proposal by the T2S Board within a reasonable amount of time, taking into account the urgency of the Change Request. The T2S Board submits a proposal to the Governing Council after having reached a consensus with the CSG and the NECSG taking into account the advice of the AG in accordance with paragraph 8.
8. If consensus cannot be achieved based on the stakeholders’ initial resolutions, the T2S Board aims at reconciling the different views before the Governing Council takes its final decision:

a. The T2S Board coordinates discussions with relevant stakeholder groups in order to find a consensual solution. The T2S Board may ask for a re-assessment of the Change Request by the CRG taking into account the views of all relevant stakeholders. Based on the CRG re-assessment, the T2S Board discusses with all relevant stakeholder groups taking into account respective views and prepares a compromise proposal within a reasonable amount of time, taking into account the urgency of the Change Request. The T2S Board shares this proposal with the CSG, the NECSG and the AG. For issues of key concern, this consensus driven approach to establish a compromise proposal may be a repetitive process. Once consensus is reached within a reasonable amount of time, taking into account the urgency of the Change Request, the AG formally gives its new advice and the CSG and the NECSG take new resolutions on the Change Request.

b. If such discussions do not lead to consensus, the T2S Board, the CSG or the NECSG may ask for a non-binding external advice except for matters related to safeguarding the integrity of currencies in T2S or to financial stability. The party providing such advice needs to be selected by common agreement of the T2S Board, the CSG and the NECSG and deliver its advice in parallel to the T2S Board, the CSG, the NECSG and the AG. All relevant stakeholder groups review their position on the basis of the non-binding external advice and the T2S Board coordinates discussions with the relevant stakeholder groups in order to find a consensual solution in accordance with paragraph 8a. Within a reasonable amount of time and taking into account the urgency of the Change Request, the AG formally gives its final advice and the CSG and the NECSG take final resolutions on the Change Request before the Governing Council takes the final decision on the basis of a proposal by the T2S Board.

9. The final decision of the Governing Council is published on the T2S’s website.

10. The Contracting CSD and Participating CSDs have the right to challenge the final decision of the Governing Council before the Court of Justice of the European Union.

1.3 Decision-making on relevant matters other than Change Requests

1. Any individual Participating CSD, the Contracting CSD, euro area NCB, non-euro area NCB, the ECB, the 4CB or User member in the AG may, outside the scope of Change
Requests, propose a resolution or, in particular in the case of the AG, an advice concerning relevant matters of T2S\(^1\) to the T2S Board or, in exceptional circumstances, to the Governing Council.

2. In all Governance bodies the chairperson may decide that the proposal for a resolution or an advice needs first to be analysed by a substructure, i.e. a technical group (permanent) or by a task force (ad-hoc). The T2S Board or, in exceptional circumstances, the Governing Council organises the procedure in such a way that all Governance bodies are properly consulted within a reasonable amount of time and without duplicating substructures on similar topics. In case of divergence of views between different Governance bodies, the T2S Board shall aim at reconciling the different views. The CSG or the NECSG can, upon agreement with the T2S Board, ask for a non-binding external advice for relevant matters of T2S\(^1\) except for matters related to safeguarding the integrity of currencies in T2S or to financial stability. The party providing such advice needs to be selected by common agreement of the T2S Board, the CSG and the NECSG and shall deliver its advice in parallel to the T2S Board, the AG, the CSG and the NECSG.

3. A decision on the proposal is taken by the Governing Council or, for matters which have been delegated by the Governing Council, by the T2S Board after consultation of the AG, the CSG and the NECSG within a reasonable amount of time, taking into account the urgency of the matter. Differing views between the Eurosystem and non-euro area NCBs are dealt with according to the relevant procedure defined in the Currency Participation Agreement. The decision of the Governing Council or the T2S Board shall be published on the T2S website.

4. The Contracting CSD and Participating CSDs have the right to challenge the final decision of the Governing Council before the Court of Justice of the European Union.

\(^1\) Such relevant matters include crisis management, risk issues, operational issues, monitoring the T2S Service (in accordance with the Service Level Agreement), pricing issues, acceptance for testing and go-live.
2 Additional Governance arrangements

In addition to the general Governance procedures outlined above, this section clarifies a number of specific situations.

2.1 Prioritisation

The Change Review Group:

- shall assess Change Requests and prepare a list of ranked Change Requests based on the procedures described in Schedule 9 (Change and Release Management).

The Project Managers Group:

- shall prepare a prioritisation proposal for defining the content of a T2S release based on the procedures described in Schedule 9 (Change and Release Management).

The AG:

- shall submit its advice regarding the prioritisation of Change Requests to the T2S Board;

The CSG:

- shall make a resolution addressed to the T2S Board regarding the prioritisation of Change Requests stemming from the Contracting CSD, Participating CSDs or in relation to the functioning rules of Securities Accounts;

- may prepare a proposal to the T2S Board on the prioritisation of all Change Requests.

The NECSG:

- shall make a resolution addressed to the T2S Board regarding the prioritisation of Change Requests stemming from the non-euro area NCBs or in relation to the functioning rules of Dedicated Cash Accounts;

- may prepare a proposal to the T2S Board on the prioritisation of all Change Requests.

The T2S Board:
shall prepare a proposal for the prioritisation of all T2S Stakeholder Change Requests to be submitted to the Governing Council taking into account the views of the AG, the CSG and the NECSG. If the proposals for prioritisation of Change Requests provided by the T2S Board, the AG, the CSG and the NECSG diverge, the T2S Board shall aim at finding consensus and seeks the views of the AG, the CSG and the NECSG before submitting the final proposal on the prioritisation of Change Requests to the Governing Council.

The Governing Council shall:

- prioritise all T2S Stakeholder Change Requests, on the basis of a T2S Board proposal, to which the views obtained from the AG, the CSG and the NECSG are attached.

2.2 Changes driven by Legal and Regulatory Requirements

Changes motivated by Legal and Regulatory Requirements shall be dealt with according to the standard procedure set out in Schedule 9 (Change and Release Management) with high priority, in accordance with Principle [4] of the General Principles of T2S, and following the relevant decision-making process. Such Change Requests have to be initiated by the affected entities. However, several cases have to be distinguished:

(a) Changes in European legislation are dealt with as quickly as possible or as required in the legislation. The analysis of the Change Request by the various Governance bodies mentioned in this note concerns only the modalities of the implementation.

(b) It is expected that the Contracting CSD and Participating CSDs and Central Banks inform the T2S Board on any proposed change in national legislation with an impact on T2S as early as reasonably practicable. The relevant Change Requests shall be dealt with according to the standard procedure. The final decision shall be taken by the Governing Council and a potential refusal shall include the reasons why the implementation of the Change Request is not feasible.

(c) Change Requests resulting from a Relevant Competent Authority request shall follow the standard procedure and the Eurosystem shall involve the AG, the CSG and the NECSG. Should these discussions lead to a disagreement with the Relevant Competent Authority, the Change Request shall be brought to the Governing Council and the Relevant Competent Authority will be invited to submit its written view directly to the Governing Council. The Governing Council would then take due account of the views of the Relevant
Schedule 8 – Governance

211 Competent Authority before making a decision. Should the Governing Council reject the Change Request, it will provide a written explanation of the rationale to the Relevant Competent Authority. The Governing Council can reconsider its decision based on additional information provided by the Relevant Competent Authority. When a Change Request resulting from a Relevant Competent Authority request relates to only one market, it shall not be in contradiction with the General Principles of T2S and relevant costs shall be borne by the CSDs, i.e. the Contracting CSD and/or Participating CSDs, subject to the regulatory decision.

219 (d) Changes under (b) and (c) above which involve legislation or regulatory requirements in a non-euro area country are discussed in the Governors’ Forum, if the Governor of the relevant non-euro area NCB so requests.

222 The Eurosystem shall aim at finding solutions to the cases outlined above, including the possibility of optional features to the extent that they are technically viable and within the Lean Scope of T2S.

2.3 Transparency

226 In order to allow a wide range of market participants to remain closely involved in T2S developments, the extensive T2S transparency regime shall be continued and relevant documentation and information shall be made available on the T2S’s website. In particular, the Eurosystem’s offer of the future updates of the Framework Agreement to all interested CSDs and of the Currency Participation Agreement to all interested non-euro area NCBs shall be made transparent. Furthermore, relevant advice, resolutions and decisions related to changes shall be published. This transparency will allow all T2S Stakeholders to contribute to ongoing T2S discussions and make their views known to relevant Governance bodies.

2.4 Technical groups supporting the Governance bodies

235 Each Governance body has the possibility to establish technical groups, and to dissolve them, to deal with T2S issues that are within its remit. The T2S Board shall make proposals to avoid duplication of substructures on similar topics.

238 The technical groups shall in particular:

239 (a) ensure that T2S and subsequent releases go-live and that CSDs, as well as Central Banks, are duly and timely prepared, including with regard to the relevant aspects of User Testing and Migration;
(b) review, in line with Schedule 2 (T2S Programme Planning and Monitoring), the CSD-relevant planning and programme reporting, including risks and issues;

(c) assess Change Requests, as defined in Schedule 9 (Change and Release Management);

(d) develop and maintain the Manual of Operational Procedures; and

(e) meet the Eurosystem to review the T2S service performance against the SLA.

The technical groups shall report to the relevant Governance bodies. The technical groups have the possibility to exchange relevant information directly among themselves. They organise their work in an efficient manner to fulfil their mandates, including the possible creation of their own substructures.

At the time of the signature of the Framework Agreement, the following groups have been considered as technical groups:

(a) PMG: Project Managers Group, established by the Steering Level and consisting of project managers of the Contracting CSDs and Participating CSDs, euro area NCBs, non-euro area NCBs, the ECB and 4CB. The T2S Board shall appoint the chairperson of the PMG on the basis of her/his technical expertise after consultation of the CSG and the NECSG. The PMG reports to the T2S Board and keeps the CSG and the NECSG informed of its work. It needs to ensure that T2S and subsequent releases go live and that CSDs as well as Central Banks are duly and timely prepared. Its name, mandate and need for continuation will be reviewed when all CSDs and Central Banks will have migrated to T2S.

(b) CRG: Change Review Group, established by the Steering Level and consisting of product managers and functional experts of the Contracting CSD and Participating CSDs, euro area NCBs, non-euro area NCBs, the ECB and 4CB. User representatives participate in the CRG as observers. The T2S Board shall appoint the chairperson of the CRG on the basis of her/his technical expertise after consultation of the CSG and the NECSG. The CRG reports to the CSG via the ECB. The ECB disseminates the deliverables of the CRG also to the T2S Board, the AG and the NECSG. It assesses Change Requests as defined in Schedule 9 (Change and Release Management). The CRG and the PMG also need to exchange information regarding the impact of changes on the T2S timeline. The CRG continues the work of the AG Sub-Group on User Requirements Management.
OMG: Operations Managers Group, established by the Steering Level and consisting of operations experts of the Contracting CSD and Participating CSDs, euro area NCBs, non-euro area NCBs, the ECB and 4CB. Representatives of Users which are Directly Connected Parties participate in the OMG as observers for specific agenda items. The T2S Board shall appoint the chairperson of the OMG on the basis of her/his technical expertise after consultation of the CSG and the NECSG. The OMG reports to the T2S Board and informs the AG, the CSG and the NECSG. It develops and maintains the Manual of Operational Procedures, meets to review the T2S Service performance against the SLA and coordinates the management of operational incidents. The OMG continues the work of the AG Sub-Group on Operational Framework.
Annex - Mandate of the CSG

1 Preamble and Objectives

The TARGET2-Securities (T2S) Services that the Eurosystem offers to Central Securities Depositories (CSDs) in Europe allow for the core, neutral and borderless settlement of securities transactions on a Delivery versus Payment basis in Central Bank Money. This is performed in a single technical platform integrated with Central Banks’ Real-Time Gross Settlement systems for all participating currencies.

The Governing Council and the CSDs signing the Framework Agreement (FA) and thus participating in T2S (hereinafter the ‘Participating CSDs’) agree to establish the CSD Steering Group (CSG). The CSG discusses all matters of relevance for Participating CSDs. The CSG supports the decision-making process in the multilateral T2S Service by providing the Eurosystem with the CSDs’ common position on matters of relevance for Participating CSDs. The CSG works within the ‘Governance’ specified in Schedule 8 of the FA.

2 Responsibilities and Tasks

The CSG is responsible for articulating and coordinating the views of Participating CSDs within the T2S Governance. It is the T2S Governance body which, with respect to a set of matters stipulated in the FA, makes resolutions and gives advice on behalf of the Participating CSDs.

The CSG has the possibility to give its advice or agree on a resolution on any issue related to T2S. The CSG gives its advice and makes resolutions in particular on:

- any issue brought to the Governing Council that has implications for the FA;
- changes to the FA and its Schedules, in line with the applicable procedures;
- issues of major interest concerning T2S;
- changes to the T2S Scope Defining Set of Documents, in line with the applicable procedures specified in the FA Schedule 8 (Governance) and Schedule 9 (Change and Release Management);
- the prioritisation of Change Requests stemming from Participating CSDs;
Schedule 8 – Annex – Mandate of the CSG

- material subcontracting;
- disputes between the Eurosystem and non-euro area NCBs upon the invitation of the T2S Board, the Governing Council or the NECSG;
- any other consultation request of the T2S Board or the Governing Council;
- crisis management;
- risk issues;
- operational issues;
- monitoring the T2S Service (in accordance with the Service Level Agreement);
- pricing issues;
- acceptance for testing and go-live, and
- on any matters of relevance in relation to the FA.

On all other matters having an impact on the Participating CSDs, the CSG is informed about envisaged decisions of the Governing Council or the T2S Board and the CSG shall be provided with sufficient time to formulate any objections it may have.

A disagreement between one or more Participating CSD and the Eurosystem can be escalated from the working and sub-structure level to the CSG and shall follow the dispute resolution and escalation procedure specified in Article 42 of the FA. The dispute resolution and escalation procedure does not preclude a subsequent Arbitration procedure pursuant to Article 43 of the FA.

3 Composition and Term

The CSG is composed of:

- as full members, the CEOs/members of the managing board of Participating CSDs/groups of Participating CSDs that have signed the FA;
- up to six User representatives, as observers, proposed by the T2S Board and nominated by the Governing Council for a renewable term of two years, based on applications from the European Banking Federation (EBF), the European Savings Bank Group (ESBG), the European Association of Co-operative Banks (EACB), the Association for Financial
4 Reporting

The CSG gives its advice and makes resolutions to the T2S Board as the managing body of T2S, upon invitation or on its own initiative. The T2S Board establishes procedures to inform other T2S Governance bodies of relevant CSG resolutions and advice. The CSG may send its resolutions directly to the Governing Council if the CSG considers that the General Principles of T2S or other core elements of T2S are at risk. The CSG may seek the advice of the T2S Advisory Group.

5 Working Procedures

Detailed working procedures are to be specified in the ‘Rules of Procedure’ drafted by the CSG and endorsed by the Governing Council.

Any member of the CSG may propose a resolution or an advice. CSG resolutions and advice are subject to a double majority, defined as the simple majority of the Participating CSDs, provided that they represent at least 75% of securities settlement transactions in T2S.

As a rule, the CSG meets once every quarter. Additional meetings may be called by the CSG Chairperson, the dates of which are communicated sufficiently in advance to the CSG. In principle, meetings take place at the ECB’s premises. The ECB provides operational and secretarial support to the CSG.
The CSG may establish technical groups to support its work if considered necessary. It coordinates with the T2S Board who organises the work in such a way that all relevant Governance bodies are properly involved without duplicating technical groups on similar topics.

As part of the transparency principle of T2S, CSG resolutions and advice are in general published on T2S’s website.
FRAMEWORK AGREEMENT

SCHEDULE 9

CHANGE AND RELEASE MANAGEMENT
INTRODUCTION

1 OBJECTIVE

2 SCOPE

3 ENTITIES INVOLVED IN THE CRM PROCESS

3.1 TECHNICAL LEVEL

3.1.1 ECB

3.1.2 4CB

3.1.3 Participating CSDs and the Central Banks

3.1.4 Change Review Group (CRG)

3.1.5 Project Managers Group (PMG)

3.1.6 Operations Managers Group (OMG)

3.2 STEERING LEVEL

4 CHANGE MANAGEMENT

4.1 CATEGORISATION OF CHANGES

4.1.1 Type of change according to urgency

4.1.2 Type of change according to beneficiary

4.1.3 Parameters of changes

4.1.3.1 Parameter 1: Legal/business importance

4.1.3.2 Parameter 2: Market implementation efforts

4.1.3.3 Parameter 3: Operational/technical impact

4.1.3.4 Parameter 4: Financial impact for T2S

4.2 CHANGE MANAGEMENT PROCESS

4.2.1 Change Request Initiation and Registration

4.2.2 Preliminary assessment

4.2.3 Authorisation

5 RELEASE MANAGEMENT

5.1 RELEASE TYPES AND FREQUENCY

5.2 RELEASE MANAGEMENT PROCESS

5.2.1 Definition of release
Schedule 9 – Change and Release Management

5.2.2 Release baselining ........................................................................................................ 23
5.2.3 Release monitoring..................................................................................................... 23
5.2.4 Implementation ......................................................................................................... 24
5.2.4.1 Design, building and configuration ...................................................................... 25
5.2.4.2 Testing of a new release by the Participating CSDs and the CBs ......................... 25
5.2.4.3 Roll-out and communication ................................................................................ 28
5.2.4.4 Delivery – Go-live .............................................................................................. 29
5.2.5 Post implementation review .................................................................................... 29

ANNEX 1 - CHANGE REQUEST FORM ................................................................. 1
ANNEX 2 - CHANGE REQUEST STATUS .............................................................. 3
Introduction

There will be changes in T2S for a variety of reasons. Due to the fact that these changes need to be translated in a timely and consistent way into functional, legal, operational or technical specifications, with the involvement of (and impact on) all relevant T2S stakeholders, a proper Change and Release Management process (CRM) must be defined and implemented. In addition, the implementation of any of these changes can risk damaging the service’s availability or integrity, and may require changes (or specific monitoring efforts) on the part of entities connected to, or relying on, T2S. The CRM process is thus essential in order to efficiently track and manage changes to T2S and to mitigate the risks associated with these changes.

The definition of a release will follow a demand driven model, meaning that a priority rating is used to establish the order in which the authorised changes should be considered for a particular T2S release, and also taking into consideration the available capacity and the resources for implementing the change. The CRM process is based on the ITIL (Information Technology Infrastructure Library) framework version 3.0 for IT service management.

The CRM process will apply before and after T2S Go-Live Date, for all Change Requests (falling within the scope of this document) that are initiated as from the entry into force of the Framework Agreement respectively the Currency Participation Agreement.

The Eurosystem, the CSDs that have signed the Framework Agreement (FA) (‘Participating CSDs’) and the non-euro area NCBs that have signed the Currency Participation Agreement (CPA) (‘connected non-euro area NCBs’) will be entitled to participate in the CRM process as full members of the technical groups in accordance with the T2S Governance. User representatives participate in the CRG as observers.

Meanwhile, the CSDs and non-euro area NCBs which have not yet entered into an agreement with the Eurosystem by the agreed date will have no right of co-decision in the CRM process until they sign. They will be kept informed about the changes to the T2S Services via T2S communication channels.
1 Objective

The objectives of the CRM process are to:

- Respond to the relevant T2S Stakeholders’ changing business requirements while maximising value and minimise the risk of change related incidents;

- Ensure that Change Requests falling within the scope of this document will be managed within the Lean Scope of T2S;

- Ensure that Change Requests are managed in an efficient and controlled manner from the initiation until implementation (recorded and then evaluated, authorized, and that the resulting changes are prioritized, planned, tested, implemented, documented and reviewed in a controlled manner);

- Ensure that Change Requests falling within the scope of this document are communicated to all relevant T2S Stakeholders in accordance with the rules laid down in this Schedule and in Schedule 8 (Governance);

- Agree on the exact T2S release content and plan the successful rollout of a release into the production environment; and

- Ensure that all changes are traceable, secure and that only correct, authorised and tested versions are installed on the T2S production environment.
2 Scope

The CRM process applies to

- all functional changes which trigger any addition to, deletion from or modification of any item in T2S as defined in the T2S Scope Defining Set of Documents\(^1\), as well as to changes to these documents, even if they do not have an impact on the T2S functionality;

- the requirements to be fulfilled by NSPs, as laid down in – and taking into account the provisions of – the Licence Agreement, and to the specifications for the Value-added Connectivity Services necessary to implement the Dedicated Link Connections; and

- non-functional changes that affect T2S functionality: they are modifications to the technical platform on which T2S operates, or to the T2S software that do not change the functionality, but their implementation potentially impacts the interoperability and services of CSDs, Central Banks and/or Directly Connected Parties (DCPs). An example for this category of change would be an upgrade of the database software that would require testing by CSDs and Central Banks prior to its implementation in production.

The General Principles of T2S in Section 1.2 of the User Requirements Document cannot be changed as a by-product of another Change Request, but only by a separate Change Request to the General Principles of T2S, which follows the decision-making process in this Schedule and respecting the Eurosystem rights as described in Schedule 8 (Governance). If any other Change Request falling within the scope of this Schedule is not in line with the General Principles of T2S as they read from time to time in the User Requirements Document, the CRG will immediately report such inconsistency to the Steering Level and wait for guidance before continuing the assessment of that Change Request.

Any change subject to the CRM process must be undertaken following the process outlined in this document.

Corrections/changes covered by maintenance activities for fixing errors, mistakes, failures or faults in the software system, which produce an incorrect or unexpected result, or cause it to behave in unintended ways (e.g. fixing errors in coding, design or detailed specification,

---

\(^1\) The T2S Scope Defining Set of Documents as defined in the Schedule 1 (Definitions) to the FA and the CPA.
performing changes to the system caused by an incident/problem) will be managed according to the procedures defined in the Manual of Operational Procedures. However, although these corrections/changes do not need assessment and authorisation in the context of Change Management process, they follow the Release Management process as described in chapter 5.2.

The following changes are not subject to the CRM process:

- Technical changes to hardware/infrastructure components (i.e. non-functional changes without impact on the T2S functionality) under the control of the Eurosystem that are necessary to sustain the daily operation of T2S in accordance with the Service Levels specified in Schedule 6 (T2S Service Level Agreement). The respective arrangements/procedures for handling these changes are covered in Schedule 6 (T2S Service Level Agreement) and will be detailed in the Manual of Operational Procedures. The operational body/team responsible for managing and implementing the technical changes should liaise closely with the Change Review Group (as defined in section 3.1.3) to ensure a smooth implementation, in particular in case of technical changes that may have an impact on the service delivered (based on the risk assessment); Business configuration changes related to market parameters that can be done by the Participating CSDs/CBs or by the Eurosystem in accordance with the procedures defined in the Manual of Operational Procedures;

- Changes related to non-functional and non-technical documentation e.g. Manual of Operational Procedures, Registration and Connectivity Guides, training materials, etc;

- Updates of the baseline version of Other T2S Specification Documents and T2S Operational Phase Documents, which follow a Deliverable Change Process. The process and the substructure involved are defined in Schedule 2 Annex 8 (T2S Deliverables list and management process) to the FA and CPA.; and

---

2 In accordance with the Preamble D of the Framework Agreement, the Participating CSDs shall retain full control of the parameter of its business operations. This applies e.g. for Participating CSDs for setting up the T2S Securities Accounts for their customers including all needed access rules, granting of access privileges, etc. Setting up of these parameters and rules should be done according to the best market practices and the relevant regulatory requirements.

3 Other T2S Specification Documents and T2S Operational Phase Documents as defined in the Schedule 1 (Definitions) to the FA and the CPA and in the Schedule 2 Annex 8 (T2S Deliverables list and management process).
Other changes related to the FA and its annexes, respectively to the CPA and its annexes that will be managed according to the relevant procedure as set out in the FA, respectively the CPA or the relevant annex following the applicable Governance regime.
3 Entities involved in the CRM process

There are two levels differentiated in the CRM process: a “technical” level and a “Steering” Level. The Participating CSDs and the Central Banks are expected to organise themselves according to these two levels.

3.1 Technical level

3.1.1 ECB

The T2S Team of the ECB supports the T2S Board in the CRM process. The roles and responsibilities of the ECB at the different stages of the CRM process are described in the chapters 4.2 and 5.2 of this Schedule. They include, inter alia:

- being the entry point for all Change Requests;
- keep a register of all Change Requests;
- manage their processing as described in this document;
- monitor Change Requests during their entire lifecycle, from the initiation until they have reached their end status (i.e. authorization or rejection);
- monitor the release definition and its implementation;
- track progress and issues that may influence decision-making and report them inter alia to the Change Review Group; and
- ensure availability of the relevant information to the relevant T2S Stakeholders.

3.1.2 4CB

4CB means the Deutsche Bundesbank, the Banco de España, the Banque de France and the Banca d’Italia, collectively, in their capacity as NCBs responsible for building, maintaining and running the T2S Platform based on the respective contractual arrangements and on decisions of the Governing Council. In the context of CRM process, the 4CB is entrusted with different roles
and responsibilities as described in the chapters 4.2 and 5.2 of this Schedule. They include, inter alia:

- assess the impact stemming from requests for new functionalities or technical enhancements from a technical, functional and operational point of view (feasibility, planning, budget);
- building, configuration and delivery of a release into production;
- propose the time-frame for implementing a change or a release; and
- examine the impact on the system security and provide a security impact assessment.

### 3.1.3 Participating CSDs and the Central Banks

The euro area NCBs, the Participating CSDs and the connected non-euro area NCBs are entitled to participate in the CRM process. Their roles and responsibilities at different stages of the CRM process are described in the chapters 4.2 and 5.2 of this Schedule. They include inter alia:

- act as full members of the Change Review Group (CRG);
- initiate Change Requests on their own or customers’ behalf;
- evaluate and monitor Change Requests;
- monitor release definition and implementation;
- test and verify releases; and
- involve their respective user communities in the process.

### 3.1.4 Change Review Group (CRG)

With regard to CRM the CRG will be responsible, inter alia for/ in charge of:

- reviewing Change Requests on regular basis, evaluate the information provided in the Change Request and in the assessment (checking its consistency and completeness across all Change Requests) and making proposals for decision making at the Steering Level;
building and maintaining the scoring mechanism according to which authorised changes
will be ranked in view of their implementation in (one of) the next release(s); and
reviewing the content of each release as well as any changes to the agreed release.

As regards the interactions with the Steering Level, the role of the CRG is limited to managing
the process from reviewing and evaluating the Change Request to making proposal for its
authorisation/rejection as well as the ranking of authorised changes based on the scoring
mechanism. The CRG will aim at reaching a common agreement in making a proposal to the
Steering Level for their decision-making. In case of disagreement, both majority and minority
views will be reported to the Steering Level. Once the decision to authorise the content of a T2S release has been taken, the decision is binding for the CRG’s further work.

The CRG reports to the CSG via the ECB. The ECB also provides the deliverables of the CRG to
the T2S Board, the AG and the NECSG.

The CRG will be informed and – to the extent possible and relevant – consulted on technical
changes and changes that need to be implemented urgently in order to restore and continue the
provision of T2S Services, by the relevant operational groups responsible for handling these
changes, in accordance with the procedures defined in the Manual of Operational Procedures.

The CRG will schedule regular meetings, typically every 2 months, but meetings can also be
organised more frequently if deemed necessary. The CRG should have face-to-face meetings,
however some of the assessment process can be handled in written procedure if this process is
accepted by the CRG in advance.

3.1.5 Project Managers Group (PMG)

With regard to CRM, inter alia, the PMG will be responsible for:

- preparing the plan for implementation of T2S releases;
- coordinating and monitoring the implementation of T2S releases;
- providing a T2S release scope for approval to the T2S Steering Level based on the list of
  ranked and assessed change requests from the CRG and the list of ranked and assessed
  production problems from the OMG;

4 The authorisation of a Change Request is covered in the chapter 4.2.3
reviewing and monitoring the content of each release as well as any changes to the agreed T2S release scope.

3.1.6 Operations Managers Group (OMG)

With regard to CRM, inter alia, the OMG will be responsible for:

- assessing and ranking production problems that are pending resolution; and
- reviewing the content of each release as well as any changes to the agreed T2S release scope.

3.2 Steering Level

Without prejudice to the role of the Governing Council, the governance bodies at the Steering Level are (i) the T2S Board, (ii) the CSD Steering Group (CSG) and (iii) the Non-euro Currencies Steering Group (NECSG) as defined in the FA and the CPA.

Their roles and responsibilities in the decision-making process of changes and in the prioritisation of Change Requests for defining the content of the next T2S releases, as well as the escalation and dispute resolution procedure in case of disagreement between the Participating CSDs and the Eurosystem, or between the non-euro area NCBs and the Eurosystem are described in the FA, the CPA and Schedule 8 (Governance).

Each governance body at the Steering Level will receive information from the technical groups via the ECB with respect to the CRM process. In the spirit of transparency, this information will also be shared with the Advisory Group in accordance with Schedule 8 (Governance).
4 Change management

4.1 Categorisation of changes

4.1.1 Type of change according to urgency

According to its level of urgency, a change falls under one of the following categories:

- **Normal changes**: changes that can be planned without time constraints and will go through the CRM process before being implemented into the production environment.

- **Fast-track Changes**: changes that are imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management, or changes that are critical for the stability of the T2S Platform or imposed by Central Bank decisions related to safeguarding the currency/-ies or related to crisis management measures to ensure financial stability and that, owing to the time constraints, have to be implemented in a shorter timeframe than normal, which will be decided on an ad-hoc basis. These changes will also go through the CRM process, however, the length of the different process steps will be shortened on an ad-hoc basis, in particular for preliminary and detailed assessment. The CRG may also provide a recommendation to the PMG to coordinate the allocation to a release and the detailed assessment without requiring a preliminary assessment in case of a fast-track change.

4.1.2 Type of change according to beneficiary

Irrespective of the urgency, all changes subject to the CRM process fall into one of the following categories:

- **Common Changes**: any new feature, functionality or service – or any amendment of an existing feature, functionality or service –which is implemented for the benefit of all T2S Actors.

- **Specific Changes**: any new feature, functionality or service – or any amendment of an existing feature, functionality or service – which is not implemented as a Common Change (within the applicable Governance arrangements), but which some Participating
CSDs and/or CBs wish to implement, provided that it is compliant with the Lean Scope of T2S, and for which they jointly accept to bear the investment and running costs. In case of Specific Change i) the unauthorised use should be either controlled or monitored (as agreed in the request). ii) in order to avoid any impact on non-supporting Participating CSDs/CBs, the implementation mechanism will be based – if possible – on the approach that the functionality will be made available to all parties, but that those not wishing to use it, are not impacted by the change. iii) If this backward compatibility cannot be ensured, the change can only be authorised upon agreement of each non-supporting CSD/CB. These changes may be triggered by:

- market-specific regulatory, legal, fiscal or market-specific requirements or,
- innovation or improvement considered useful by one or more Participating CSDs or CBs.

### 4.1.3 Parameters of changes

Each change is categorised based on a number of parameters which are used to indicate how important or delicate a change is relative to others changes.

#### 4.1.3.1 Parameter 1: Legal/business importance

The importance of a Change Request derives from the business need for a change and should be part of the business justification. From an importance viewpoint, the Change Requests will be classified into one of four categories as defined below:

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>1) A change required by the Eurosystem or by a connected non-euro area NCB to implement its statutory tasks.</td>
</tr>
<tr>
<td></td>
<td>2) A change relating to an area which would - if the change is not implemented - prevent Participating CSDs or CBs or their customers from connecting to and/or using T2S or put the requester in non-compliance (after implementing any work-arounds) with legal, regulatory (including, among others, unacceptable operational risks), or fiscal requirements.</td>
</tr>
</tbody>
</table>
### Schedule 9 – Change and Release Management

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
</table>
| High | Changes that would offer a significant enhancement and benefits to the T2S Service or the T2S Actors.  
2) A change to embody agreed harmonisation in T2S where there is a high efficiency benefit.  
3) A change to significantly improve safety or stability.  
4) A change to remove major ambiguity or inconsistency in the T2S Scope Defining Set of Documents or the T2S Documentation. |
| Medium | 1) A change with moderate efficiency benefits, but which does not have an important harmonisation dimension.  
2) A change to improve the usability of the system.  
3) A change to remove minor ambiguity or inconsistency in the technical and functional documentation. |
| Low | 1) Changes that are “nice to have” and are useful to pad out a release.  
2) A change to improve clarity of the technical and functional documentation. |

#### 4.1.3.2 Parameter 2: Market implementation efforts

Change Requests will be classified into three categories on the basis of the effort required by the market to properly implement and timely absorb the change (i.e. implement the necessary IT changes, adapt the operational procedures, integrate the change into the service offerings, adapt the legal arrangements, etc.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Changes that require high efforts (a long implementation time and significant resources) on the side of the majority of Participating CSDs, CBs and/or their communities in order for them to be able to implement the change and take full benefit</td>
</tr>
</tbody>
</table>
of it.

**Medium**

Changes that require high efforts (a long implementation time or significant resources) on the side of a minority of Participating CSDs, CBs and/or their communities or medium efforts on the side of the majority of Participating CSDs, CBs and/or their communities in order for them to be able to implement the change and take full benefit of it.

**Low**

Changes that do not require a long implementation time and any significant resources on the side of Participating CSDs, CBs and their communities in order for them to be able to take full benefit of the change.

4.1.3.3 **Parameter 3: Operational/technical impact**

Change Requests will be classified into three categories on the basis of the operational/technical impact if the change is undertaken, i.e. the risk that a change might trigger (some) instability on the T2S Platform. The technical/operational risk of a change is its potential undesirable/unexpected adverse impact on the T2S Platform and on the CSD/CBs.

<table>
<thead>
<tr>
<th>Category</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High</strong></td>
<td>Changes that have the potential to significantly threaten the Service Level for a significant part of T2S Services or have a significant operational impact on the Participating CSDs, CBs or 4CB, because insufficient mitigating measures can be taken.</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Changes that have the potential to significantly threaten the Service Level for a minor part of T2S Services or have a limited operational impact on the Participating CSDs, CBs or 4CB, because insufficient mitigating measures can be taken.</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Changes that are expected not to threaten the Service Level for Participating CSDs or CBs or to have no or insignificant operational impact on the Participating CSDs, CBs or 4CB.</td>
</tr>
</tbody>
</table>
4.1.3.4 Parameter 4: Financial impact for T2S

An indication of the impact of the change on the required cost will be provided by the 4CB during the preliminary assessment phase. During the detailed assessment phase, the 4CB will provide the precise investment cost and the annual running cost, including a breakdown on costs for hardware, software and telecommunication.

Change Requests will be classified into five categories on the basis of the cost impact for the implementation of the Change Request.

<table>
<thead>
<tr>
<th>Category</th>
<th>Financial Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>Changes with an investment cost of at least 700 000 EUR</td>
</tr>
<tr>
<td>High</td>
<td>Changes with an investment cost of at least 400 000 EUR, but less than 700 000 EUR</td>
</tr>
<tr>
<td>Medium</td>
<td>Changes with an investment cost of at least 200 000 EUR, but less than 400 000 EUR</td>
</tr>
<tr>
<td>Low-medium</td>
<td>Changes with an investment cost of at least 100 000 EUR, but less than 200 000 EUR</td>
</tr>
<tr>
<td>Low</td>
<td>Changes with an investment cost of less than 100 000 EUR</td>
</tr>
</tbody>
</table>
4.2 Change Management process

All changes defined in chapter 2 as falling within the scope of the CRM process are subject to the Change Management (CM) process, the principles of which this section describes. The detailed description of Change Management is documented in the T2S Operational Governance Process Framework, which is listed in the Annex to Schedule 2 of the FA and CPA as a T2S deliverable.

4.2.1 Change Request Initiation and Registration

The requester, i.e. Participating CSDs, euro area NCBs, connected non-euro area NCBs, the ECB or the 4CB, can submit a Change Request to the ECB using the standard form attached in Annex 1 (Change Request Form) and supply key information such as the title of the requested change, its description (changes in the existing features and functionalities, new features and functionalities in T2S), its business motivation (including the legal/regulatory requirement\(^5\)), the urgency of the change, the categorisation of change, the date of the request, etc.

Users will always initiate Change Requests indirectly via a Participating CSD or a Central Bank. If this is not successful, Users can propose the initiation of a Change Request as a resolution in the AG. Then upon agreement of the AG, the Change Request is submitted for registration to the ECB who will submit it to the CRG for consideration according to the process described in this chapter.

The requester should clearly state in the description of the change whether the change should be implemented as a Specific Change and whether the unauthorised use of the Specific Change should be prevented or monitored.

Upon receipt the ECB will check the proposed Change Request for formal completeness, collect any missing information from the requester, register the Change Request and confirm its receipt to the requester. The ECB will submit the registered Change Request to the CRG to perform a formal validation. The CRG will check the clarity and completeness of the request, that no complementary changes will be required for its implementation, confirm if the change should be assessed as a Specific Change and/or as a Common Change considering the interest expressed by

---

\(^5\) Changes which are motivated by Legal and Regulatory Requirements will be implemented according to chapter 2.2 of Schedule 8 (Governance).
the other Participating CSDs/ CBs and agree carrying on with the preliminary assessment. After the CRG’s validation, the registered Change Request will be published on the website\(^6\).

### 4.2.2 Preliminary assessment

Upon the agreement of the CRG to carry out the preliminary assessment, the ECB and the 4CB will perform a preliminary assessment of the proposed Change Request.

The preliminary assessment includes:

- **compliance check**: whether it falls within the Lean Scope of T2S and does not conflict with another Change Request already submitted;

- **functional assessment**: how does it affect the functionality as described in the T2S Scope Defining Set of Documents;

- **technical assessment**: evaluate the technical feasibility and complexity, analyse which domains, business sub-areas or other RTGS and /or CMS systems will be impacted. If necessary, the ECB will cooperate with the relevant non-euro area NCBs and consult the relevant ESCB committees or business areas that are responsible for these Eurosystem services;

- **cost assessment**: preliminary indication of the impact of the change from a cost perspective (see Parameter 4 in chapter 4.1.3.4 above); and

- **risk assessment**: whether it could trigger instability to the T2S Platform or create performance problems.

The result of the preliminary assessment will be provided by the ECB to the CRG for evaluation, in average 6 weeks and maximum 8 weeks from the agreement of the CRG to carry out the preliminary assessment.

While preliminary assessment is conducted by the ECB and 4CB, the Participating CSDs and CBs will consult their user communities in order to collect information on the change benefits.

---

\(^6\) If the Change Request relates to safeguarding the integrity of the respective currency and/or financial stability as part of crisis management measures, transparency could be limited to the contracting T2S Actors upon request of a Central Bank.
and its impact on the process on the Users’ side. This will allow the Users to provide their input and ensure that T2S provides functionality according to the needs of the market.

The CRG will review the outcome of the preliminary assessment and, based on that, provide a recommendation to the Steering Level on whether to authorise or reject the Change Request for inclusion in the ranking procedure.

The CRG may also decide to reject a change request after preliminary assessment. This requires the agreement of the requester, in which case the process stops at this stage. The governance bodies at the Steering Level will be informed accordingly. If there is a disagreement from the requester, the issue is escalated to the Steering Level for guidance.

4.2.3 Authorisation

The Steering Level authorises or rejects a Change Request in accordance with Schedule 8 (Governance). The Steering Level may request further evaluation to be conducted by the CRG in order to complement the overall picture. In that case, the impacts of the Change Request will be re-assessed/evaluated as described in chapter 4.2.2.

The final decision on the Change Request may be:

1. To reject the Change Request. If all Participating CSDs and CBs agree on this decision then the process stops at this stage.

2. To authorise the change, as well as its cost recovery method, according to the principles specified in Schedule 7 (Pricing) to the FA and the CPA.

If a change is authorised after a failed dispute resolution in the Governors’ Forum, which triggers the termination of the CPA by a non-euro area NCB, the latter has the right to exit T2S within a maximum period of 24 months. During this time and to the extent relevant for the operation of T2S, the non-euro area NCB shall not be affected by the change that triggered their termination.

If such a change is imposed by a competent EU authority, the concerned CB will either make its best endeavours for a quicker exit, or will make the necessary changes in its system so that T2S can implement the change.

The final decision of the Governing Council shall be published on the T2S website. Once authorised, the Change Request will become part of the list of authorised changes, and hence
become eligible for implementation in (one of) the next T2S release(s), as explained in chapter 5 on the Release Management process.
5 Release management

The Release Management (RM) process ensures that all aspects of a change, technical and non-technical, are considered together. The main objective is to deliver, distribute and track one or more changes intended for simultaneous release into the live environment while protecting the integrity of the production environment and its services.

The RM process covers the planning, design, build, configuration and testing of software and hardware to create a set of release components for the production environment. The term “Release” is used to describe a collection of authorised changes which typically consist of enhancements to the T2S Service (i.e. new and/or changed software required and any new or changed hardware needed for the implementation of the changes) and a number of production problem resolutions which are implemented into the production environment.

The goal of the RM process is to ensure that authorised changes and the production problem resolutions that have been agreed as part of a release are secure and traceable, and that only correct, tested and authorised versions are installed into the production environment.

All authorised changes initiated via a Change Management process and the production problem resolutions shall follow the RM process.

5.1 Release types and frequency

As of the T2S Go-Live Date the releases can be classified as follows:

- Major release: a release that consists of a set of software changes that affect a significant part of the functionality or that adds substantial new functionality. It may also include the resolution of identified production problems.

- Minor release: a release that encompasses a set of software changes to align with the regularly scheduled update of the ISO 20022 message standard, and, when feasible, to implement a limited number of Change Requests that do not affect a significant part of the functionality. It may also include the resolution of identified production problems.

- Fast-track release: if T2S is confronted with changes that are imposed by Legal and Regulatory Requirements, or by CSG resolutions related to risk management, or changes
that are critical for the stability of the T2S Platform or imposed by Central Bank

decisions related to safeguarding the currency/-ies or related to crisis management

measures to ensure financial stability that cannot be bundled into the next major or

minor release due to the time constrains, T2S will have to comply with these

requirements, possibly with an additional release, typically containing only the relevant

change(s).

- Production problem release: it includes the resolution of identified production problems

which cannot be planned for the next major or minor release.

After the T2S Go-Live Date given the active involvement required from various relevant T2S

Stakeholders over a certain period of time, the frequency of releases should be minimised in

order to be able to manage risks adequately. The optimum frequency of releases should be

balanced between the business requirements and the relative impact, risk and cost of the release.

Consequently, depending on needs and resource allocation, and without prejudice to the need for

any fast-track releases, the Eurosystem can support every year: one major release and - in case of

need - one minor release and two production problem releases to resolve those identified

production problems which cannot be planned for the next major or minor release.

The Participating CSDs and CBs will have the possibility to monitor the release implementation

and to carry out the testing according to the provisions currently described in Schedule 2 (T2S

Programme Planning and Monitoring) and 3 (User Testing) to the FA and to the CPA.  

5.2 Release Management process

This chapter describes the principles of the RM process that applies to all authorised Change

Requests and production problem resolutions. The detailed description of Release Management is

documented in the T2S Operational Governance Process Framework, which is listed in the

Annex to Schedule 2 of the FA and CPA as a T2S deliverable.

5.2.1 Definition of release

Based on the lists of authorised changes, the CRG will examine each Change Request in detail

and will propose a ranking of these changes based on a scoring mechanism. The detailed

---

*Footnote: If required, the Schedule 2 and 3 will be reviewed and amended after the T2S Go-Live Date release in order to adapt them to the upcoming releases.*
The description of the process according to which authorised Change Requests will be scored is documented in the Scoring Mechanism, which is listed in the Annex to Schedule 2 of the FA and CPA as a T2S deliverable. Similarly, the OMG will assess and rank all production problems that are pending resolution.

When conducting the ranking exercise, the CRG should consider the following criteria for Common Changes:

- to ensure a level playing field for all T2S Stakeholders in order to create the highest possible level of satisfaction throughout all T2S Actors/for each type of stakeholders’ point of view;
- to consider those changes that bring benefits to the wide majority of the Participating CSDs and CBs; and
- to select those changes which in total serve the interest of all Participating CSDs and CBs.

The CRG should also consider the following criteria for Specific Changes:

- to assess the changes with the aim of balancing the ratio of Common and Specific Changes;
- to select those Specific Changes requested by the Participating CSDs/CBs that do not benefit to a large extent from the Common Changes; and
- to increase the priority of Specific Changes in proportion to the time they are waiting to be implemented.

Based on the outcome of the ranking exercises, the PMG will prepare its proposal on the content of the next T2S release.

The ECB and 4CB will prepare detailed assessments for those Change Requests and feasibility assessments for those production problem resolutions included in the T2S release scope proposal of the PMG.

In the detailed assessment the impact of the Change Requests will be evaluated based on the following dimensions:

---

8 Excluding those changes that are frozen during the exit time of a non-euro area NCB (see chapter 4.2.3)
Framework Agreement

Schedule 9 – Change and Release Management

**Functional impact** – to evaluate the functional consequences of a change, which function(s) it impacts.

**Technical impact** – to evaluate the technical consequences of a change, which module it impacts, the possible impacts on market participants, the complexity of the change, etc.

**Cost impact** - the assessment of the costs in order to implement the feature. The financial impact will cover the precise investment cost and the annual running costs as well as a breakdown of costs for hardware, software and telecommunication.

**Legal impact** - to evaluate possible impact of the Change Request on the legal construction of T2S and to assess any legal, regulatory or fiscal requirements – particularly on the Participating CSDs and CBs concerned, as well as Intellectual Property Rights-related issues.

**Service Level impact** – to evaluate the impact on the Service Level, including the KPIs agreed with the Participating CSDs, CBs and the other T2S Users.

**Documentation impact** - assessment of the documents that will need to be modified as a result of the Change Request. This can be the URD, GFS, UDFS, GS, GTD, Service Description, the GUI Business Functionality, User Handbooks, SLA, MOP etc.

**Impact on the security of the system** – to examine the impact on the system security and draw the attention to any risk that the Change Request would create.

**Impact on operations** – to highlight any constraint that the Change Request may impose directly or indirectly on IT operations and the possible resulting technical, operational or financial impacts.

The detailed assessment takes a maximum of 10 weeks for the ECB and 4CB after the decision to conduct the detailed assessment has been taken. Each Change Request shall be analysed without undue delay and assuring the quality.

The Eurosystem will provide justification when a Change Request cannot be implemented in a release due to lack of adapting its capacity. The Eurosystem will make best efforts to adapt its capacity to manage the demand for Change Requests as soon as possible.

While defining and approving the scope of a T2S release the relevant bodies may reassess and amend the initial decision to authorise a Change Request.
Based on the outcome of the above process steps following the respective order, the PMG will
provide its proposal for the T2S release scope to the T2S Steering Level after consultation with
the OMG and CRG.

In case of disagreement in the PMG, the recommendation will draw the attention of each group to
the changes relevant for them, outline the reasons for disagreement and if possible suggest a few
variants/options with respect to the release content.

5.2.2 Release baselining

In parallel to the release scope definition, the PMG will prepare a detailed service transition plan
that will ensure synchronisation with the Participating CSDs’/CBs’ planning and presents the
intended scope as well as all elements required to execute and monitor the release.

All governance bodies at the Steering Level will review the PMG proposal on the content of the
release including the related costs and the service transition plan for approval in accordance with
Schedule 8 (Governance). At the end, the Governing Council of the ECB shall prioritise all
Change Requests and take a decision on the recommended release scope and service transition
plan, on the basis of a T2S Board proposal, to which the views obtained from the CSG, the
NECSG and the AG are attached. The information on changes selected for the next T2S release
will be published on the website.

5.2.3 Release monitoring

Once the service transition plan is finalised and agreed, the PMG will manage and monitor this
plan in accordance with the provisions of Schedule 2 (T2S Programme Planning and Monitoring)
to the FA and the CPA.

In accordance with the roles and responsibilities defined in Schedule 2 (T2S Programme
Planning and Monitoring) of the FA and CPA, the following key principles will be followed in
the context of release monitoring and reporting:

- A common service transition plan for the release will be maintained based upon clearly
  identified deliverables and synchronisation points taking into account all the respective
  constraints and dependencies of the involved parties;
A regular and close monitoring of the service transition plan for the release, with decisions committing all parties will be undergone based on a comprehensive framework established to manage events that may affect the release deliverables and milestones;

- Relevant documentation and necessary information will be provided by the Eurosystem to all involved parties as background information for supporting release monitoring and reporting;

- Regular meetings will be organised between the Eurosystem and the Participating CSDs/ CBs to review and discuss the overall status assessment of the T2S release implementation, to discuss progress and any risks and issues that might jeopardize the release, and recommend mitigation measures/corrective actions;

- A reporting framework will be established by the Eurosystem to inform regularly all involved parties at the various levels of Governance about the status assessment of the release implementation, including the progress against the plan, to provide status assessment of each deliverable relevant for Participating CSDs and CBs and to ensure that the planning issues and risks are identified, discussed and addressed in a timely and appropriate manner;

- A T2S risk and issue management and reporting framework will be established by the Eurosystem to identify, manage and report of risks and issues, affecting the successful delivery of the release;

- A comprehensive framework will be established to allow the Eurosystem to monitor the readiness status of all involved parties to deliver the release into production; and

- The Participating CSDs and CBs will ensure their own readiness and coordinate the readiness of their clients to be ready to use the T2S release, i.e. ensuring planning feasibility and monitoring progress.

5.2.4 Implementation

The implementation phase starts with the designing, building and configuration through the final testing and verification stages and ends with the actual release into the production environment.
The implementation phase is initiated upon completion of the release baselining process, the principles of which are described in section 5.2.2. The release baselining process is completed at the latest one year before the planned go-live of a minor or major release. The lead time for a production problem resolution release may be less, when agreed.

5.2.4.1 Design, building and configuration

Once the approved content of the release is communicated to the 4CB, the latter will be responsible for designing, building and configuring the release. This process includes, inter alia, the following activities:

- Creating a new version of one or more software modules;
- Purchasing equipment or services externally;
- Preparing a hardware modification;
- Updating all relevant documentation or producing new one;
- Providing training to the Participating CSDs and the CBs, if required.9

The following relevant documents are updated by the ECB and 4CB depending on the release scope, and will be provided to the T2S Stakeholders at the points in time as specified in the agreed service transition plan:

- URD, GFS, UDFS, Service Description and GUI Business Functionality, GS, GTD, User handbooks, SLA, MOP

The ECB and 4CB will ensure consistency across all documentation, including legal agreements and operational procedures.

5.2.4.2 Testing of a new release by the Participating CSDs and the CBs

The Eurosystem will conduct a Eurosystem Acceptance Testing before the start of User Testing thereby ensuring that the T2S test environments and T2S Platform meet the functional and non-functional requirements (including performance testing - if there is a potential impact on the

---

9 The Participating CSDs, respectively the CBs are responsible for the providing training to their users. On Participating CSDs'/ CBs' request, the Eurosystem should agree on providing trainings for Participating CSDs' resp. CBs' users for topics selected by Participating CSDs/CBs.
performance) by the change in order for the users to successfully carry out their User Testing. 

Once the Eurosystem internal tests are finalised, the Eurosystem confirms the readiness of the T2S testing environments for the T2S User Testing via a release note. The test calendar is communicated to the Participating CSDs and the CBs providing information on the testing activities, the availability of the testing environments and any other relevant information for performing the testing. This test calendar and the test activities will follow as much as possible – and where relevant – the approach defined in Schedule 3 (User Testing).

The Participating CSDs and CBs start testing the new release once all the entry criteria for the User Testing are met. A stability period is envisaged in the pre-production where the system should be tested while running according to the Service Level Agreement. The length of this period will be decided by the PMG on a case-by-case basis. The aim of the User Testing is to ensure that the new T2S release delivers the expected services as described in the User Requirements Document, as well as the functional and non-functional specifications and to guarantee the readiness of the Participating CSDs and CBs and their communities for the migration/operation to/of the new release.

The User Testing activities are performed according to the framework agreed between the Participating CSDs/ CBs and the Eurosystem, which may include a set of user certification tests to ensure that T2S Stakeholders are able to use the new or amended functionality correctly. As a matter of fact, the verification of the release is given by the Participating CSDs and CBs once the exit criteria of the verification process have been completed successfully.

The security impact of all proposed changes to the T2S Platform should be assessed prior to delivery into production in order to check that they do not compromise the security of the T2S Platform. In this respect it is noteworthy that security should be planned and integrated from the start of development. This ensures that risk factors are adequately considered in a timely manner and prevents unnecessary costly security measures to be implemented only once the new system is operational.

The testing and release verification process by the Participating CSDs and CBs will typically take up to 3 months (i.e. for a major release).

The following principles will be applied during User Testing phase of a release:

- The scope of release User Testing covers both functional and non-functional testing;
The preparation of non-functional release user test activities is done jointly by the Eurosystem and the Participating CSDs/CBs;

The Participating CSDs and CBs shall appoint a CSD respectively CB Test Manager who will be the primary contact point for the Eurosystem for all discussions about user release testing;

The Eurosystem shall appoint a T2S Test Manager who will ensure proper coordination and exchange of information with the CSD’s and CB’s Test Manager;

The execution of non-functional release user test activities is the primary responsibility of the Eurosystem;

The Eurosystem will report to the Participating CSDs/CBs about the results of non-functional release testing;

User Testing of a new release aims at ensuring compliance of T2S with the T2S Scope Defining Set of Documents;

The Participating CSDs and CBs define their acceptance tests and agree these with the Eurosystem;

The Eurosystem defines certification tests and agrees these with the Participating CSDs and CBs;

User Testing of a new release is organised in different stages: interoperability testing (both bilateral and multilateral), acceptance testing, community testing and business day testing, based on the concept and the principles laid down in Schedule 3 (User Testing);

The Participating CSDs and CBs are responsible for the co-ordination of user test activities of a new release with their communities;

The Eurosystem is responsible for the co-ordination of user test activities of a new release between all T2S Actors, including the organisation of a central repository for test sets, test cases and test scenarios related to the certification tests for T2S User Testing;
The Eurosystem will support the User Testing activities of a new release through the implementation of incident and problem management procedures as described in the Manual of Operational Procedures;

- The Participating CSDs and CBs shall inform the Eurosystem of any incident they experience during the execution of their user tests of a new release;

- In particular, the Eurosystem shall undertake all necessary corrective measures to resolve all release defects discovered during the User Testing activities of a new release and caused by T2S;

- All decisions related to (un)succesful completion of the test stages, as well as the implementation of the release in the production environment will be prepared under the responsibility of the Project Managers Group (PMG) and will be made in accordance with the Governance arrangements laid down in Schedule 8 (Governance).

5.2.4.3 Roll-out and communication

The service transition plan drawn up during the preceding phases will be complemented with information about the exact installation process and the agreed implementation activities and delivery of the release into production.

The ECB in collaboration with the 4CB, Participating CSDs and CBs will agree on the rollout planning which includes the following:

- Producing an exact, detailed timetable of events, as well as who will do what i.e. resource plan;
- Producing the release note and communication to the Users;
- Planning communication;
- Incident management.

All the impacted T2S Stakeholders will be informed on what is planned and how it might affect them. The responsibilities of the interested parties in the implementation of the release will be communicated by the ECB ensuring that everyone is aware of them. This will be accomplished via the release communication/notes.
5.2.4.4 Delivery – Go-live

Bringing the application software release into the production environment is the final step in the Release Management process.

To ensure a smooth roll-out of the release, the checklist and procedures agreed between the Eurosystem, 4CB, the Participating CSDs and CBs need to be followed by all the involved parties.

The Governing Council shall give the formal and final acceptance of the release for the go-live based on the successful completion of the user testing of the new release and after obtaining the views of the CSG, and the NECSG. The release is delivered into the production environment on the agreed date following the agreed procedures.

5.2.5 Post implementation review

A post implementation review will take place periodically in order to evaluate the change/release performance and to verify the effectiveness of the change/release package implementation.

These review meetings will provide an opportunity to assess and review the efficiency and effectiveness of the Change and Release Management Process, as well as to identify any potential improvement to the overall process flow.
## Annex 1 - Change Request Form

### General Information

<table>
<thead>
<tr>
<th>CR raised by:</th>
<th>Institute:</th>
<th>Date raised:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Request title:</th>
<th>CR ref. no:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(to be filled in by the ECB)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Change Request type</th>
<th>Urgency</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Common, Specific, if specific unauthorised use to be controlled or monitored?):</td>
<td>(to be filled in by the requester)</td>
</tr>
<tr>
<td></td>
<td>(to be filled in by the requester)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(to be filled in by the requester)</td>
<td>(to be filled in by the requester)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(to be filled in by the requester)</td>
<td>(to be filled in by the 4CB)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requester Category (CSD, CB, ECB, 4CB)</th>
<th>Status:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(to be filled in by the requester)</td>
<td>(to be filled in by the CRG)</td>
</tr>
</tbody>
</table>

### Description of requested change:

### Reason for change and expected benefits/business motivation:
Annex 2 - Change Request Status

At any time, a Change Request will have one of the following statuses:

registered – The Change Request was registered by the ECB.

Rejected by Change Review Group – When the Change Review Group has agreed with the requester that the change should be dropped.

Under preliminary Assessment – The ECB/4CB is conducting the preliminary assessment.

Pending with Change Review Group – The ECB has submitted the preliminary assessment to the Change Review Group to review it and consult their communities.

Under Detailed Assessment – The ECB/4CB is conducting the detailed assessment of the Change Request.

Being evaluated by the Change Review Group – The ECB has submitted the detailed assessment to the CRG and they are evaluating it.

Pending at Steering Level – The Change Request with the assessment is submitted to the Steering Level for a formal authorisation.

Authorised at Steering Level – The Steering Level has authorised the change and it was placed on the official list of changes.

Rejected at Steering Level – The Steering Level has rejected the change.

Allocated to a release – The change is allocated to a release.

Under implementation – The change is under implementation but not yet delivered to test.

Delivered to test – The change is being tested by the CSDs and CBs.

Verified – The change was successfully tested and verified by the CSDs and CBs.

Parked – Change Request is parked for the next T2S release(s).

Frozen – The implementation of the change is frozen for max. 24 months due to the exit period of a non-euro area NCB.

Closed – The Change Request has been implemented in T2S and all relevant documentation has been updated and all other impacted documents have been aligned.
FRAMEWORK AGREEMENT

SCHEDULE 10

INFORMATION SECURITY
Framework Agreement
Schedule 10 – Information Security

Table of contents

1 Objective and scope of T2S Information Security ................................................................. 2
  1.1 Objective .......................................................................................................................... 2
  1.2 Scope ............................................................................................................................... 2

2 General responsibilities of the contracting parties ............................................................... 4
  2.1 General responsibilities of the Eurosystem ..................................................................... 4
  2.2 General responsibilities of the Contracting CSD ............................................................. 5

3 The T2S Information Security management framework ...................................................... 6
  3.1 The Information Security Policy for T2S ................................................................. 6
  3.2 The T2S Information Security Requirements and Controls ......................................... 6
  3.3 The T2S Information Security risk management process .............................................. 6

4 The T2S Information Security risk management process .................................................... 7
  4.1 Risk management methodology .................................................................................... 8
  4.2 Deliverables to the Contracting CSD .......................................................................... 12
  4.3 Co-operation and escalation procedures ...................................................................... 15
  4.4 Examples for the Shared Documents .......................................................................... 16

31 October 2011
Introduction

This document aims at presenting the provisions related to the framework to ensure that the requirements concerning Information Security in T2S are met and kept up-to-date. In addition the document defines the involvement of the Contracting CSD in the Information Security management process, in accordance with the applicable governance arrangements, as well as the Eurosystem’s reporting obligations towards the Contracting CSD.

The management of Information Security for T2S is largely based on the ISO/IEC standards 27001:2005 and 27002:2005. This Schedule and the related Annexes therefore use the terms and definitions of these standards, if applicable, and in such case prevail over the terms defined in Schedule 1. A definition of the relevant terms is included in chapter 2 of Annex 2 (T2S Security Requirements and Controls) to this Schedule.

The document is divided into four chapters, corresponding to the major aspects identified as relevant for T2S Information Security: i) objective and scope of T2S Information Security; ii) general responsibilities of the contracting parties; iii) the T2S Information Security management framework, and iv) the T2S Information Security risk management process.
1 Objective and scope of T2S Information Security

1.1 Objective

The objective of T2S Information Security is to protect T2S business processes and its information from a wide range of threats, whether internal or external, deliberate or accidental, and to minimise the impact on the T2S Platform of any threats, that, despite all measures taken, do materialise.

ISO 27001 defines Information Security as “preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved”\(^1\).

For the avoidance of doubt, it is acknowledged that “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” (i.e. operational risk as defined in the report entitled “International Convergence of Capital Measurement and Capital Standards”, published by the Basel Committee on Banking Supervision, June 2006), is covered by the T2S Information Security Policy, to the extent such risk may have an impact on the confidentiality, integrity and availability of T2S information. Operational risks that are not covered by the T2S Information Security Policy are covered in the SLA reports as specified in Schedule 6 (T2S Service Level Agreement).

1.2 Scope

The scope of the T2S Information Security Schedule covers all arrangements aiming at fulfilling the T2S Information Security Requirements and Controls as specified in Annex 2 (T2S Security Requirements and Controls) to this Schedule, as well as to the relevant principles to conduct the initial risk analysis before go-live and all subsequent risk analyses during the production phase. These risk analyses focus on the proper implementation of the agreed security controls. Furthermore, all reporting obligations and the activities to keep the T2S Information Security management framework up-to-date are covered by this Schedule as well.

\(^1\) ISO 27001:2005 (chapter 3.4)
The perimeter of the T2S Information Security management framework is limited to the T2S Platform and does not extend to the system(s) in place on the side of the Contracting CSD. Nevertheless, the Eurosystem commits to provide the Contracting CSD with all information necessary to allow the latter to perform its own risk management obligations. Network Service Providers are also out of scope for the T2S Information Security management framework managed by the Eurosystem, but the Eurosystem imposes certain requirements, comparable to those for Third Party service providers, via the agreements.
Framework Agreement  
Schedule 10 – Information Security

2 General responsibilities of the contracting parties

As an overarching principle, the Eurosystem and the Contracting CSD shall co-operate in good faith in order to allow both parties to fulfil their commitments with respect to Information Security.

2.1 General responsibilities of the Eurosystem

The Eurosystem shall:

a) implement the T2S Information Security management framework in accordance with this Schedule, in particular by designing, developing and operating the T2S Platform with the objective that each T2S Actor has access to T2S information according to the confidentiality, integrity and availability requirements described in this Schedule and its Annexes;

b) implement a process to manage Information Security in T2S according to the process described in section 4 of this Schedule:

a. regularly reviewing the implementation;

b. regularly updating the T2S Security Requirements and Controls to keep them in line with technical and other material developments;

c. regularly assess the effectiveness of the process and update it if necessary;

c) share the asset classification scheme and likelihood and impact grading scales used in the risk management process for information;

d) report the results of Information Security reviews to the Contracting CSD (according to section 4.3 of this Schedule);

e) report Information Security incidents (according to the definition in Annex 2 [T2S Security Requirements and Controls] to this Schedule) and the related remediation to the Contracting CSD;
f) report to the Contracting CSD newly identified threats or detected gaps that might threaten T2S Information Security, as well as any related remediation that is envisaged to address them;

g) provide all other relevant information to the Contracting CSD to allow the latter to fulfil its own risk management obligations.

2.2 General responsibilities of the Contracting CSD

In view of ensuring Information Security for T2S, the Contracting CSD shall:

a) ensure its own compliance with Information Security requirements according to its internal standards, regulatory requirements and/or best practices;

b) report Information Security incidents (according to the definition in Annex 2 [T2S Security Requirements and Controls] to this Schedule) to the Eurosystem, if T2S or other T2S Parties might be impacted by such incidents; and

c) report to the Eurosystem newly identified threats or detected gaps that might threaten T2S Information Security.
3. The T2S Information Security management framework

This chapter describes the documents that specify the Eurosystem’s commitments in the Information Security management process.

To ensure Information Security the related requirements and implemented measures need to evolve over time to accommodate for new threats and to adapt to technical and other material developments. All the annexes will therefore regularly be reviewed and if need be updated according to the arrangements specified in section 4.1.4.1 below.

3.1 The Information Security Policy for T2S

The Information Security Policy for T2S – attached as Annex 1 (Information Security Policy for T2S) to this Schedule – is a high-level document embracing, at a generic level, a definition of the scope of Information Security for T2S, the security policy principles, allocation of responsibilities and other relevant aspects related to Information Security in the T2S environment.

3.2 The T2S Information Security Requirements and Controls

The purpose of the T2S Security Requirements and Controls – attached as Annex 2 to this Schedule – is to specify which conditions are to be fulfilled (i.e. the requirements) for establishing Information Security for T2S, as well as to indicate how these conditions can be met (i.e. the controls). The requirements and controls are based directly on ISO standard 27002.

3.3 The T2S Information Security risk management process

The T2S Information Security risk management process – described in chapter 4 of this Schedule – specifies the approach for managing Information Security for T2S and the related reporting of the risk situation and planned risk treatment to the Contracting CSD.
4 The T2S Information Security risk management process

This chapter outlines the approach to ensure the continuous process of managing Information Security in T2S. This approach is established under the umbrella of the Information Security Policy for T2S (Annex 1 to Schedule 10) which embraces at a generic level a definition of the scope of T2S, the Information Security policy principles, the allocation of responsibilities and summarises the Information Security management domains.

The main goal of Information Security in T2S is to protect T2S information from a wide range of threats and to minimise the impact of any threats on T2S operations, which, despite all measures taken, do materialise. In particular, T2S Information Security aims at avoiding any propagation of Information Security incidents, whether caused endogenously in T2S or by a T2S Actor, to other T2S Actors. To accomplish this, the T2S risk management process defines two main processes. One process (i.e. the “review” process) ensures that the T2S Information Security management framework is kept up to date and effective, while the other process (the “core” process) focuses on the implementation of this framework and the assessment of any remaining risks.

A full risk assessment is performed before the initial go-live of T2S (pre-production security assessment). Moreover, the process interfaces with the Change Management and with the incident management processes to guarantee that the security requirements and controls are in place and that the risk is continuously monitored and maintained at an appropriate level. In addition to these event-driven assessments, a time-driven mechanism ensures a complete security compliance checking and risk assessment every three years also for parts that have not been subject to a change.

This chapter is structured as follows:

- Section 4.1 puts the T2S Information Security risk management process into the perspective of the complete T2S Information Security management framework;
- Section 4.2 places emphasis on the information flow exchanged between the Eurosystem and the Contracting CSD during the T2S risk assessment process cycle;
- Section 4.3 describes the co-ordination and escalation process for T2S Information Security issues and in particular how the Contracting CSD will be involved in the T2S Information Security management process;
4.1 Risk management methodology

The Information Security risk management methodology applied by the Eurosystem for T2S is defined as the series of interlinked components, which provide the common methodological foundation for delivering, maintaining and governing T2S Information Security and related internal controls for the Eurosystem.

4.1.1 Business impact analysis

Risk management commonly starts with a criticality assessment of the information system as a whole determining the business impact for the Eurosystem in relation to the three security aspects: confidentiality, integrity and availability. Since T2S plays a vital role in the post-trade services chain, and has cross-system relationships to systems at many CSDs as well as RTGS and collateral management systems of the Central Banks, it is a systemically important system. Undoubtedly, the protection needs, in terms of confidentiality, integrity and availability would reach the highest score. However, even for a highly critical system not all components are of the same criticality level. Therefore, the Eurosystem categorises the individual assets using the following inventory classification principles.

The rules being that:

- an owner is identified/nominated for each asset;
- the criticality for each asset is identified taking confidentiality, integrity and availability aspects into account;
- all the security requirements and controls (see section 4.1.2) are considered as applicable to T2S;
- deviations from this general rule is under the owner\(^2\) responsibility according to the asset classification’s criticality and the applicability of the control;

\(^2\) In accordance with ISO 27002, the term ‘asset owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner'
deviations must be justified and argued during the compliance checking phase performed by Information Security experts who have no direct or indirect conflict of interest in the performance or outcome of this compliance check.

The list of assets and their categorisation are subject to change. If changes are required to T2S due to changes in the list of assets (or their categorisation), then these updates will be performed as part of the Change and Release Management process. On top of that, the asset inventory will be subject to a complete review every three years.

4.1.2 The T2S Information Security Requirements and Controls

The list of controls taken into account for the individual assets is derived from the following different sources:

- ISO/IEC standard 27002:2005 as mentioned in the URD;
- URD chapter 18;
- Experience from Target2.

When compiling this list, all controls from all listed sources were taken into account. Only those controls that are obviously not applicable to T2S have been dropped from these inputs.

By coordinating this effort with the work done for Target2 and CCBM2, the Eurosystem ensures that a common approach for these three core systems is followed to ensure an appropriate high level of Information Security for all three interconnected systems.

4.1.3 The T2S Threat Catalogue

The T2S Threat Catalogue listing all threats that have been considered for T2S is compiled out of input taken from the Information Security forum.

The Eurosystem consolidated the input by differentiating between threats and root causes, which in itself are not a threat but can allow several threats to become imminent.

---

does not mean that the person actually has any property rights to the asset, but refers rather to “stewardship” or “custody” of assets, in particular for data.
The T2S Threat Catalogue provides information on relevant threats to the system (internal or external/accidental or deliberate) and serves as the basis for the identification of the impact, the appropriate security controls and (later) evaluation of potential residual risks.

The purpose of the T2S Threat Catalogue is twofold; it helps to identify all potential threats to T2S without overlooking any and to ensure that all threats are addressed properly by mapping the security requirements and controls to the threats they address.

4.1.4 The T2S Information Security risk management process

Information Security risk management for T2S is based on two main processes:

- The T2S Information Security management framework review process ensures that the T2S Information Security management framework continues to adequately address the risks, as they change over time by ensuring a timely update and approval of documents. The T2S Information Security management framework review process consists in identifying new and changed threats deriving from system changes and new business requirements, incidents and security developments, as well as Legal and Regulatory Requirements. In addition to this continuous, event driven process, the Eurosystem will review all documents of the T2S Information Security management framework on a yearly basis.

- The compliance and risk assessment process is used to assess the overall T2S Information Security risk situation. This includes the security compliance check to identify deviations from the T2S Information Security Requirements and Controls as well as their assessment and reporting to the CSDs and NCBs. The process applied to the whole T2S scope is triggered every three years, the first before the go-live of T2S (the pre-production security assessment). In between these full verifications, any changes to T2S or any security related incident will trigger a partial verification for the relevant parts.
Figure 1: The two risk management processes and their interaction

4.1.4.1 T2S Information Security management framework review process

The T2S Information Security management framework review process ensures that the T2S Information Security management framework continues to adequately address the risks that T2S is exposed to, as they change over time. The findings resulting from Change Requests, incidents and security developments provide the Eurosystem with information on which to base a sound decision on whether the relevant documents, i.e. the Information Security Policy for T2S, the T2S Threat Catalogue and the T2S Security Requirements and Controls, should be updated.

In addition to this continuous, event driven process, the Eurosystem will review all documents of the T2S Information Security management framework on a yearly basis.

If the need for an update to the Information Security Policy or to this Schedule is identified, an updated version of the document(s) is proposed to the relevant governance body (as defined in
Schedule 8 [Governance] for approval. In addition, the CSG and the NECSG will be consulted on any proposed changes to the T2S Security Requirements and Controls. Changes to other documents defining the Information Security framework are made unilaterally by the Eurosystem.

4.1.4.2 Compliance and risk assessment process

The compliance and risk assessment is a multi-step process to assess the overall risk situation.

In a first step (security compliance check), it takes the defined security requirements and controls and performs a compliance check by validating the completeness and effectiveness of the actual implementation of these controls within the scope of T2S.

In a second step (risk assessment), all threats addressed by non-compliant controls are assessed (based on grading scales) concerning likelihood of the risk materialising and its associated impact.

In a third step, the risk situation of T2S concerning each threat is determined by aggregating the results of the individual assessments for those controls that are relevant for this threat into an overall likelihood and potential impact. The result is represented using a grading scale.

In a fourth step, the Eurosystem will make a proposal for the treatment of all identified risks based on their potential impact on the Eurosystem as provider of the T2S Services. Available options to treat risks are acceptance, avoidance, mitigation or transfer of risks.

In a final step, for all risks that cannot be or are not accepted, actions plans for avoiding, mitigating or transferring the risks will be defined and implemented (risk treatment plan – see section 4.2.2).

4.2 Deliverables to the Contracting CSD

The Eurosystem drives the process described in section 4.1. However, the assessment of the risk impacts can only be based on the impact on T2S and/or the Eurosystem. This section therefore focuses on the information the Eurosystem will share with the Contracting CSD and their options to use this as input to their own business risk assessment processes in order to meet their regulatory requirements and to get evidence that the security requirements are addressed properly by the Eurosystem.
### T2S Information Security Risk Evaluation Table

The ‘T2S Information Security Risk Evaluation Table’ (ISRET) is generated as part of the risk assessment. It provides the likelihood for each threat for which not all the relevant controls are implemented and effective, as well as the impact of the threat, taking into account the non-compliant controls. The ISRET includes the following information:

1. **ID**: Threat identification number
2. **Threat**: Threat description (from the Threat Catalogue)
3. **Current likelihood**: (based on a likelihood grading scale)
4. **Likelihood explanation**: explanation of the likelihood scoring
5. **Current impact**: (based on an impact grading scale)
6. **Impact explanation**: explanation of the impact scoring
7. **Risk treatment plan ID**: reference to the appropriate treatment plan mitigating the risk, as described in the T2S Information Security risk treatment plan (see section 4.2.2)

Based on this ISRET, the Contracting CSD has the necessary information to evaluate its own business risk.

Section 4.4.1 shows the template and an example of this table.

The Eurosystem will share with the Contracting CSD the ISRET whenever it is updated, but at least on a yearly basis.

### T2S Information Security risk treatment plan

Together with each ISRET, the Eurosystem will share the proposal for the ‘T2S Information Security Risk Treatment Plan’ (ISRTP).

This plan proposes a treatment (i.e. a mitigation measure or acceptance) for all the risks listed in the ISRET.
Framework Agreement
Schedule 10 – Information Security

The ISRTP includes the following information:

1. Risk treatment plan ID: Risk treatment plan identification.
2. Proposed treatment: information on the planned safeguard measures or proposal to accept the risk together with an explanation why it is recommended to accept the risk.
3. Current likelihood of residual risk: likelihood of the residual risk before the implementation of the plan (as it appears in the ISRET).
4. Likelihood of residual risk after fix: likelihood of the residual risk after the implementation of the safeguard measures.
5. Current Impact of Residual Risk: impact of the residual risk before the implementation of the plan (as it appears in the ISRET).
6. Impact of Residual Risk after fix: impact of the residual risk after the implementation of the safeguard measures.
7. Planned Implementation Date: a deadline by when these measures will be implemented.
8. Status: Progress of the action plan implementation (not started, in progress, closed) including the date.

Mitigation measures that imply a functional change to T2S will be processed according to Schedule 9 (Change and Release Management), while mitigation measures that imply a non-functional change will be processed according to Schedule 6 (T2S Service Level Agreement – Annex 1 [Management of non-functional changes]). Should the Contracting CSD see the need for additional mitigation measures, they can as well raise Change Requests to implement these measures in T2S.

Those risks appearing in subsequent ISRTPs that require follow-up are consolidated in a single Action Plan in order to monitor whether the action plans are delivered on time. Progress monitoring on the action plans will be delivered to the Contracting CSD at least on an annual basis, and whenever there is an update to the plan or a change of status of a risk treatment (e.g. it is successfully implemented).
4.3 Co-operation and escalation procedures

The Eurosystem shall set up a multilateral co-ordination substructure, in accordance with the T2S governance, for the coordination and monitoring of the T2S Information Security risk management activities. This substructure shall meet on a regular basis and shall consist of a limited number of representatives from the Eurosystem, 4CB, CSDs and non-euro area NCBs.

The role of the substructure in charge of T2S Information Security Risk management shall be to:

- Monitor the implementation of the ISRTP;
- Review the ISRET;
- Discuss issues raised by the members of the substructure, including Information Security issues emerging outside the scope T2S Information Security;
- Prepare communications related to Information Security risks to the various T2S Stakeholders and the public at large.

If a new Information Security risk is identified, or if an existing Information Security risk obtains a higher likelihood or impact score, the Eurosystem will communicate such changes to the Contracting CSD in accordance with the incident response times specified in Schedule 6 (T2S Service Level Agreement).

Upon reception of such communication, or if another Information Security issue requires urgent attention:

- The Contracting CSD may request a conference call with the Eurosystem, at the latest during the next Settlement Day, or at its earliest convenience;
- The issue shall be discussed during the conference call;
- The Eurosystem shall summarize the outcome of the conference call and distribute it to the members of the substructure in charge of Information Security risk management.

In case no agreement can be reached in the substructure, each party shall be entitled to escalate the problem to the Project Managers Group (PMG), where the situation shall be discussed and rapidly assessed.
If a mutually agreeable solution cannot be found in the PMG, then the general T2S escalation process shall apply whereby the issue is escalated to the Steering Level in order to receive guidance to resolve the issue. The escalation process shall be in accordance with the general T2S governance arrangements, as specified in the Schedule 8 (Governance).

Ultimately there shall be recourse to the dispute resolution process as described in the provisions of the relevant Articles in the core Framework Agreement.

4.4 Examples for the Shared Documents

4.4.1 T2S Information Security Risk Evaluation Table

Example for the T2S Information Security Risk Evaluation Table that the Eurosystem will share with the Contracting CSD.

<table>
<thead>
<tr>
<th>ID</th>
<th>Threat</th>
<th>Risk Likelihood Score</th>
<th>Risk Likelihood Explanation</th>
<th>Risk Impact Score</th>
<th>Risk Impact Explanation</th>
<th>Risk treatment plan ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>Loss of historical information</td>
<td>3</td>
<td>2</td>
<td>RTP #1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>External staff dependency</td>
<td>1</td>
<td>3</td>
<td>RTP #2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>Eavesdropping</td>
<td>2</td>
<td>1</td>
<td>RTP #3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>Intentional security loopholes</td>
<td>2</td>
<td>2</td>
<td>No additional measure can be applied efficiently</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


**Framework Agreement**

**Schedule 10 – Information Security**

4.4.2  **T2S Information Security Risk Treatment Plan**

Example for the T2S Information Security Risk Treatment Plan the Eurosystem will propose to the Contracting CSD.

<table>
<thead>
<tr>
<th>Risk Treatment Plan ID</th>
<th>Description of Planned Actions / Proposal to accept the risk</th>
<th>Current Likelihood&lt;sup&gt;3&lt;/sup&gt;</th>
<th>Likelihood after fix&lt;sup&gt;4&lt;/sup&gt;</th>
<th>Current Impact&lt;sup&gt;5&lt;/sup&gt;</th>
<th>Impact after fix&lt;sup&gt;6&lt;/sup&gt;</th>
<th>Planned Implementation Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTP #1</td>
<td>Description of Risk Treatment Plan #1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>Planned date for RTP#1</td>
<td>Ongoing</td>
</tr>
<tr>
<td>RTP #2</td>
<td>Description of Risk Treatment Plan #2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>Planned date for RTP#2</td>
<td>Not started due to XXX</td>
</tr>
<tr>
<td>RTP #3</td>
<td>Description of Risk Treatment Plan #3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>Planned date for RTP#3</td>
<td>Not started</td>
</tr>
</tbody>
</table>

---

<sup>3</sup> This column provides for each threat, its likelihood for materializing before the action plan implementation.

<sup>4</sup> This column provides the likelihood of materialising for each threat influenced by the action plan (after the action plan implementation).

<sup>5</sup> This column provides the impact of each threat before the action plan implementation.

<sup>6</sup> This column provides the impact of each threat after the action plan implementation.
FRAMEWORK AGREEMENT

ANNEX 1 TO SCHEDULE 10

INFORMATION SECURITY POLICY FOR T2S
### Framework Agreement

#### Schedule 10 - Annex 1 - Information Security Policy for T2S

**Table of contents**

1. Information security management .................................................................1
2. Purpose of the T2S Information Security policy ..............................................2
3. Objective ........................................................................................................2
4. Scope of the T2S Information Security policy ...............................................3
5. Management domains of Information Security .............................................4
   5.1 Organization of information security ..........................................................4
   5.2 Asset management .....................................................................................5
   5.3 Human resources security .........................................................................5
   5.4 Physical and environmental security ..........................................................5
   5.5 Communications and operations management ............................................5
   5.6 Access control ............................................................................................5
   5.7 Information systems acquisition, development and maintenance ............5
   5.8 Information Security incident management .............................................6
   5.9 Business continuity management .............................................................6
   5.10 Compliance ...............................................................................................6
6. Responsibilities for Information Security management in T2S .....................6
   6.1 The Eurosystem .........................................................................................7
      6.1.1 Governing Council of the ECB .............................................................7
   6.2 External stakeholders ...............................................................................7
      6.2.1 Central Banks .....................................................................................7
      6.2.2 Central Securities Depositories (CSDs) ..............................................7
      6.2.3 Third Party service providers ............................................................8
Information Security policy for T2S

T2S is a service to support central securities depositaries (CSDs) by providing core, borderless and neutral settlement of securities transactions. The objective is to achieve harmonised and commoditised Delivery-versus-Payment settlement in Central Bank Money in substantially all securities in Europe.

Through its direct cross-system relationship with RTGS systems and collateral management systems, a T2S security failure might have systemic implications at a global scale. T2S is a critical IT platform supporting systemically important systems and services and should consequently be designed and operated with a high degree of security and operational reliability. Hence Information Security is a vital and integral part of T2S.

The main objective of Information Security is to protect T2S information from a wide range of threats and to minimise the impact of any threats on the continuity of T2S operations, which, despite all measures taken, do materialise. In particular, T2S Information Security aims at avoiding any propagation of Information Security incidents, whether caused endogenously in T2S or by a T2S Actor, to other T2S Actors.

Any non-compliance with the security objectives defined in the present policy note may have serious business, financial and/or reputational consequences for the Eurosystem.

1 Information Security management

Information Security management shall mean the continuous process of identifying potential threats, verifying whether security controls are comprehensive and effective and minimising or addressing security risks in line with a pre-defined risk tolerance.

Security controls selected to reduce the risk situation must be understandable, effective and – beyond those that are imposed by Legal and Regulatory Requirements – appropriate from a cost-benefit perspective. In this respect the task of Information Security management is to find an adequate balance between expenditure on controls and the business harm likely to result from security failures.

Information Security is achieved by implementing
suitable security controls. In this context it is important to note that Information Security is not only based on technical solutions. The organisational framework is equally important. In order to meet these basic principles a comprehensive T2S Information Security management framework has been developed. This framework has a hierarchical, three-layer structure ranging from a high-level policy to operational procedures. The first layer comprises an Information Security policy for T2S (i.e. the present document, in the following referred to as 'the policy'), which embraces at a generic level the security principles and further relevant aspects related to Information Security management. In the second layer, the T2S Security Requirements and Controls are specified. In the third layer, the T2S Information Security Management Manual describes in detail the Information Security management processes.

2 Purpose of the T2S Information Security policy

The policy represents the first layer of a comprehensive T2S Information Security management framework. It is a high-level document embracing, at a generic level, a definition of the scope of T2S, the security policy principles, allocation of responsibilities and other relevant aspects related to Information Security in the T2S environment. By approving the policy, the Eurosystem, in its role as owner of T2S, sets a clear direction and demonstrates its support for and commitment to Information Security. Moreover, the importance and value of T2S and its processing resources, both human and technical, are being acknowledged.

3 Objective

The main objective of Information Security is to protect T2S business processes and its information from a wide range of threats, whether internal or external, deliberate or accidental, and to minimise the impact on the continuity of T2S business of any threats that, despite all measures taken, do materialise. ISO 27001 defines Information Security as “preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved”.

---

1 The policy for T2S takes into account the “Recommendations for securities settlement systems” (Recommendation XI) published by the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions in November 2001, the ISO/IEC standard 27002:2005 and the ESCB information systems security policy.
The terms Confidentiality, Integrity and Availability are then further specified as follows:\(^2\)

- Confidentiality: the property that the asset information is not made available or disclosed to unauthorized individuals, entities, or processes;
- Integrity: the property of safeguarding the accuracy and completeness of information assets;
- Availability: the property of the asset information being accessible and usable upon demand by an authorized individual, entity, or process.

Any non-compliance with these objectives might prevent the Eurosystem from meeting its statutory business goals and/or have serious financial and/or reputational consequences. Through its direct cross-system relationship with RTGS systems and collateral management systems, a T2S security failure might, in the worst case, even have systemic risk implications at a global scale.

In order to meet the key objectives an effective Information Security management framework shall be in place.

### 4 Scope of the T2S Information Security policy

The scope of this policy comprises all assets (including human resources) needed to develop, implement, maintain and operate T2S. T2S can in principle be subdivided into the following three main layers:

1. The *infrastructure* layer, consisting of all hardware components (including interfaces), required for the development, implementation, maintenance and operation of T2S, even if these components are used, in whole or in part, for the provision of IT services outside the T2S context.\(^3\)

2. The *application* layer consisting of all software components necessary to develop, implement, maintain and operate T2S. The software component essentially consists of “the” T2S application, which is subdivided into six functional domains: Interface, Static Data Management, Settlement, Life Cycle Management and Matching, Liquidity Management and, SQRA\(^4\).

---


\(^3\) It is important to note that, in accordance with the ECB Governing Council’s decision of 8 March 2007, “the T2S service will be developed internally within the Eurosystem and operated on the TARGET2 platform in order to exploit synergies with TARGET2 to the fullest extent”. Because of this so-called “T2S on TARGET2” concept T2S infrastructure assets will exploit full benefits from the information security features already in place for TARGET2.

\(^4\) Statistics, Queries, Reports and legal Archiving
3. The *data* layer consisting of all configuration data, as well as Static and Transactional Data necessary to run T2S.

4. The *operational* layer, consisting of all procedures to be applied by and between all relevant stakeholders in order to run and complete the T2S business day in a sound and safe manner.

The smooth operation of T2S as a whole relies to some extent on secure and resilient services provided by entities which are outside the T2S boundaries. These are:

- Central Securities Depositories (CSDs).
- Central Banks allowing their currency to be settled in T2S (through the connection with their RTGS and, where relevant, collateral management systems);
- Third Party service providers (such as Network Service Providers), although the agreements between the Eurosystem and Third Party service providers are subject to the requirements specified in section 5.2.3 of Annex 2 to Schedule 10 (Information Security);

The ultimate responsibility to apply this policy to all T2S assets rests with the Eurosystem (as defined in chapter 6.1). For the assets under the control of external stakeholders (as defined in chapter 6.2) specific arrangements apply, which are established, implemented and maintained under their full responsibility (without prejudice to any minimum requirements agreed between these external stakeholders and the Eurosystem.

5 Management domains of Information Security

In the following sections the management domains of Information Security are presented. These represent at a high level the security requirements that shall be implemented in T2S in order to preserve confidentiality, integrity and availability. The specific control objectives and the security controls that shall be implemented to meet these objectives are specified in the “T2S Security Requirements and Controls” document (Annex 2 of Schedule 10).

5.1 Organization of Information Security

In order to ensure that Information Security is adequately managed an organisational framework shall be established to address Information Security related issues in a comprehensive and effective manner.

---

5 They are aligned with the high-level security requirements defined in the T2S user requirements (Chapter 18) approved by the Governing Council in July 2008.
Framework Agreement

Schedule 10 - Annex 1 - Information Security Policy for T2S

5.2 Asset management

All T2S information assets shall be identified, classified and prioritised in order to indicate the required level of protection. The responsibilities for maintaining these assets shall be clearly assigned to ensure that information assets receive an appropriate level of protection.

5.3 Human resources security

Personnel (including external party staff) shall be informed about their Information Security responsibilities, made aware about security rules and procedures and their obligation to adhere to them.

5.4 Physical and environmental security

Critical and sensitive information processing facilities shall be housed in secure areas physically protected to prevent unauthorised access to business premises, damage or compromise of information assets, interruption to business activities and theft.

5.5 Communications and operations management

Responsibilities shall be clearly allocated and procedures for the management and operation of T2S information processing facilities established in order to ensure the correct and secure operation.

5.6 Access control

Information shall be protected against unauthorised access. Access to information, information processing facilities and business processes shall be granted and controlled on the basis of business and security requirements according to the “business-need-to-know” principle.

5.7 Information systems acquisition, development and maintenance

Security requirements shall be identified and agreed prior to the development of or changes to T2S. Adequate security controls shall be in place to prevent loss, modification or misuse of information in applications systems.
5.8 Information Security incident management

Effective Information Security incident management procedures shall be in place to ensure that security events and weaknesses associated with T2S are communicated in a manner allowing timely corrective actions to be taken.

5.9 Business continuity management

A business continuity management programme shall be implemented to ensure that necessary steps are taken to identify the potential impact of security failures on the business, maintain viable recovery strategies and plans, and ensure continuity of services through training, exercising, maintenance and review.

5.10 Compliance

All relevant statutory, regulatory and contractual requirements applicable to the T2S shall be identified, documented and compliance with these arrangements shall be checked in order to avoid a breach of any criminal or civil law.

CSDs outsource a critical part of their business operations to T2S. Hence it shall be ensured that, without prejudice to any internationally recognised standards and regulations (e.g. CPSS/IOSCO), T2S is operated in compliance with the jurisdiction of the countries where the CSDs are located.

Tools and measures to ensure auditability shall be implemented.

6 Responsibilities for Information Security management in T2S

Information Security management is a key element of any sound governance structure.

The common governance structure of T2S comprises a number of different stakeholders whose roles and responsibilities with respect to Information Security are outlined in the following. In this regard, these stakeholders are either the Eurosystem or external entities (namely, the Central banks, the Central Securities Depositaries, and Third Party service providers).
6.1 The Eurosystem

6.1.1 Governing Council of the ECB

The TS2 platform is fully owned and operated by the Eurosystem [see T2S user requirements - Principle 1]. The Eurosystem is responsible for safeguarding the public function of T2S and has consequently the ultimate responsibility for deciding on the general security policy and framework for T2S Information Security management (in accordance with the User Requirements), and the definition of the risk tolerance.

In accordance with ISO 27002, the term ‘asset owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. Consequently, and without prejudice to the provisions of section 4.3 of Schedule 10 (Information Security), the Eurosystem is also responsible for defining and implementing an effective organisational framework to address Information Security issues, and for the acceptance of remaining risks. Furthermore it is responsible for verifying that all requirements specified in the Information Security policy for T2S are fulfilled in T2S.

6.2 External stakeholders

6.2.1 Central Banks

Central Banks operating national infrastructure used as interface to the T2S and providers of cash accounts are directly responsible for ensuring that Information Security is properly addressed, security controls are effective, and their personnel adhere to their internal security rules and procedures.

6.2.2 Central Securities Depositories (CSDs)

From an Information Security perspective the roles and responsibilities of CSDs are twofold.

First, an operational failure at a CSD could have a significant adverse effect on the smooth functioning of T2S. Consequently it shall be the responsibility of the CSD to ensure that their internal systems (incl. interfaces) are operated with a high degree of security and operational reliability. The relevant provisions must be addressed in the corresponding Service Level Agreement (SLA).

6 The term ‘owner’ does not mean that the person actually has any property rights to the asset, but refers rather to “stewardship” or “custody” of assets, in particular for data.
Second, CSDs are subject to a regulatory framework. In this respect CDSs shall seek assurance that T2S is providing settlement services in a secure and robust manner in compliance with applicable regulatory arrangements. To the extent that an evolution in regulatory arrangements has an impact on the T2S Platform, on the T2S Scope Defining Set of Documents, or on the T2S Specifications, these should be managed through the Change Management procedure laid down in Schedule 9.

6.2.3 Third Party service providers

Bound by contract Third Party service providers shall implement appropriate measures designed to protect against risks that could potentially result in substantial harm in terms of confidentiality, integrity and availability to any T2S Services. The relevant provisions must be addressed in the contract.
FRAMEWORK AGREEMENT

ANNEX 2 TO SCHEDULE 10
SECURITY REQUIREMENTS AND CONTROLS
## Table of Contents

1 **Introduction** 1

2 **Terms and definitions** 2
   2.1 Terms 2
   2.2 Definitions 7

3 **Structure of the security requirements and controls** 9

4 **Security policy** 10
   4.1 Information security policy 10
      4.1.1 Information security policy document 10
      4.1.2 Review of the information security policy 11

5 **Organising information security** 12
   5.1 Internal organisation 12
      5.1.1 Management commitment to information security 13
      5.1.2 Information security co-ordination 13
      5.1.3 Allocation of information security responsibilities 14
      5.1.4 Confidentiality agreements 14
      5.1.5 Contact with authorities 15
      5.1.6 Contact with special interest groups 15
      5.1.7 Independent review of information security 16
      5.1.8 Authorisation process for information processing facilities 16
   5.2 External parties 17
      5.2.1 Identification of risks related to external parties 17
      5.2.2 Addressing security when dealing with the customer 19
      5.2.3 Addressing security in third party agreements 19

6 **Asset management** 22
   6.1 Responsibility for assets 22
      6.1.1 Inventory of assets 22
      6.1.2 Ownership of assets 23
      6.1.3 Acceptable use of assets 23
   6.2 Information classification 24

19 March 2014
6.2.1 Classification guidelines 24
6.2.2 Information labelling and handling 24

7 Human resources security 25
7.1 Prior to employment 25
7.1.1 Roles and responsibilities 25
7.1.2 Screening 25
7.1.3 Terms and conditions of employment 26
7.2 During employment 27
7.2.1 Management responsibilities 27
7.2.2 Information security awareness, education, and training 28
7.2.3 Disciplinary process 28
7.3 Termination or change of employment 28
7.3.1 Termination responsibilities 28
7.3.2 Return of assets 29
7.3.3 Removal of access rights 29

8 Physical and environmental security 30
8.1 Secure areas 30
8.1.1 Physical security perimeter 30
8.1.2 Physical entry controls 31
8.1.3 Securing offices, rooms, and facilities 32
8.1.4 Protecting against external and environmental threats 32
8.1.5 Working in secure areas 32
8.1.6 Public access, delivery, and loading areas 33
8.2 Equipment security 33
8.2.1 Equipment siting and protection 34
8.2.2 Supporting utilities 34
8.2.3 Cabling security 35
8.2.4 Equipment maintenance 36
8.2.5 Security of equipment off-premises 36
8.2.6 Secure disposal or re-use of equipment 37
8.2.7 Removal of property 37

9 Communications and operations management 37
9.1 Operational procedures and responsibilities 37
9.1.1 Documented operating procedures
9.1.2 Change management
9.1.3 Segregation of duties
9.1.4 Separation of development, test, and operational facilities

9.2 Third party service delivery management
9.2.1 Service delivery
9.2.2 Monitoring and review of third party services
9.2.3 Managing changes to third party services

9.3 System planning and acceptance
9.3.1 Capacity management
9.3.2 System acceptance

9.4 Protection against malicious and mobile code
9.4.1 Controls against malicious code
9.4.2 Controls against mobile code

9.5 Back-up
9.5.1 Information backup

9.6 Network security management
9.6.1 Network controls
9.6.2 Security of network services

9.7 Media handling
9.7.1 Management of removable media
9.7.2 Disposal of media
9.7.3 Information handling procedures
9.7.4 Security of system documentation

9.8 Exchange of information and software
9.8.1 Information exchange policies and procedures
9.8.2 Exchange agreements
9.8.3 Physical media in transit
9.8.4 Electronic messaging
9.8.5 Business Information Systems

9.9 Electronic commerce services
9.9.1 Publicly available information

9.10 Monitoring
9.10.1 Audit logging 55
9.10.2 Monitoring system use 55
9.10.3 Protection of log information 56
9.10.4 Administrator and operator logs 57
9.10.5 Fault logging 57
9.10.6 Clock synchronisation 57

10. Access control 58

10.1 Business requirement for access control 58
10.1.1 Access control policy 58

10.2 User access management 59
10.2.1 User registration 59
10.2.2 Privilege management 60
10.2.3 User password management 60
10.2.4 Review of user access rights 61

10.3 User responsibilities 61
10.3.1 Password use 62
10.3.2 Unattended user equipment 62
10.3.3 Clear desk and clear screen policy 63

10.4 Network access control 63
10.4.1 Policy on use of network services 64
10.4.2 User authentication for external connections 64
10.4.3 Equipment identification in networks 65
10.4.4 Remote diagnostic and configuration port protection 65
10.4.5 Segregation in networks 66
10.4.6 Network connection control 66
10.4.7 Network routing control 66

10.5 Operating system access control 66
10.5.1 Secure log-on procedures 66
10.5.2 User identification and authentication 68
10.5.3 Password management system 68
10.5.4 Use of system utilities 69
10.5.5 Session time-out 69
10.5.6 Limitation of connection time 69
### 10.6 Application and information access control
- 10.6.1 Information access restriction
- 10.6.2 Sensitive system isolation

### 10.7 Mobile computing and teleworking
- 10.7.1 Mobile computing and communications
- 10.7.2 Teleworking

### 11 Information systems acquisition, development and maintenance

11.1 Security requirements of information systems
- 11.1.1 Security requirements analysis and specification

11.2 Correct processing in applications
- 11.2.1 Input data validation
- 11.2.2 Control of internal processing
- 11.2.3 Message integrity
- 11.2.4 Output data validation

11.3 Cryptographic controls
- 11.3.1 Policy on the use of cryptographic controls
- 11.3.2 Key management

11.4 Security of system files
- 11.4.1 Control of operational software
- 11.4.2 Protection of system test data
- 11.4.3 Access control to program source code

11.5 Security in development and support processes
- 11.5.1 Change control procedures
- 11.5.2 Technical review of applications after operating system changes
- 11.5.3 Restrictions on changes to software packages
- 11.5.4 Outsourced software development
- 11.5.5 Information leakage

11.6 Technical Vulnerability Management
- 11.6.1 Control of technical vulnerabilities

### 12 Information security incident management
- 12.1 Reporting information security events and weaknesses
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2</td>
<td>Management of information security incidents and improvements</td>
<td>86</td>
</tr>
<tr>
<td>12.2.1</td>
<td>Responsibilities and procedures</td>
<td>87</td>
</tr>
<tr>
<td>12.2.2</td>
<td>Learning from information security incidents</td>
<td>88</td>
</tr>
<tr>
<td>12.2.3</td>
<td>Collection of evidence</td>
<td>88</td>
</tr>
<tr>
<td>13</td>
<td>Business continuity management</td>
<td>88</td>
</tr>
<tr>
<td>13.1.1</td>
<td>Including information security in the business continuity management process</td>
<td>89</td>
</tr>
<tr>
<td>13.1.2</td>
<td>Business continuity and risk assessment</td>
<td>90</td>
</tr>
<tr>
<td>13.1.3</td>
<td>Developing and implementing continuity plans including information security</td>
<td>91</td>
</tr>
<tr>
<td>13.1.4</td>
<td>Business continuity planning framework</td>
<td>92</td>
</tr>
<tr>
<td>13.1.5</td>
<td>Testing, maintaining and re-assessing business continuity plans</td>
<td>93</td>
</tr>
<tr>
<td>14</td>
<td>Compliance</td>
<td>94</td>
</tr>
<tr>
<td>14.1</td>
<td>Compliance with legal requirements</td>
<td>94</td>
</tr>
<tr>
<td>14.1.1</td>
<td>Identification of applicable legislation</td>
<td>94</td>
</tr>
<tr>
<td>14.1.2</td>
<td>Intellectual property rights (IPR)</td>
<td>95</td>
</tr>
<tr>
<td>14.1.3</td>
<td>Protection of records</td>
<td>96</td>
</tr>
<tr>
<td>14.1.4</td>
<td>Data protection and privacy of personal information</td>
<td>96</td>
</tr>
<tr>
<td>14.1.5</td>
<td>Prevention of misuse of information processing facilities</td>
<td>96</td>
</tr>
<tr>
<td>14.1.6</td>
<td>Regulation of cryptographic controls</td>
<td>97</td>
</tr>
<tr>
<td>14.2</td>
<td>Compliance with security policies and technical compliance</td>
<td>97</td>
</tr>
<tr>
<td>14.2.1</td>
<td>Compliance with security policies and security requirements</td>
<td>97</td>
</tr>
<tr>
<td>14.2.2</td>
<td>Technical compliance checking</td>
<td>98</td>
</tr>
<tr>
<td>14.3</td>
<td>Information systems audit considerations</td>
<td>98</td>
</tr>
<tr>
<td>14.3.1</td>
<td>Information systems audit controls</td>
<td>98</td>
</tr>
<tr>
<td>14.3.2</td>
<td>Protection of information systems audit tools</td>
<td>99</td>
</tr>
</tbody>
</table>
1 Introduction

The purpose of the T2S security requirements and controls (T2SSRC) is to specify the security requirements for TARGET2 Securities (T2S) as laid down in the information security policy for T2S.

The T2SSRC are derived from the Information security policy for T2S and represent the second layer of the comprehensive T2S risk management framework depicted in the following exhibit.

![T2S risk management framework](image)

Exhibit 1: T2S risk management framework

As a general rule, the implementation of the security controls specified in this document is mandatory\(^1\). However, it might be that due to specific technical and/or environmental circumstances (e.g. contradicting national legislation) the application of a particular security control is not feasible. If this was the case, it will have to be justified in the context of the security assessment, more specifically when the compliance of T2S with the T2SSRC is checked, why it is not possible to implement this particular security control. The associated residual risk must then be accepted.

In addition to the requirements specified in the present document, good information systems security measures and routines corresponding to best practice (such as ISF, NIST, SANS, the German BSI) should be applied.

\(^1\) In the following document the words ‘must’ and ‘should’ are used for better readability but have the same meaning in the sense as being mandatory.
All security requirements and controls included in this document are specified from a business perspective and have to be implemented by the service provider (4CB) responsible for designing, building and operating T2S.

2 Terms and definitions

2.1 Terms

For the purpose of this document, the terms listed in the following table have the meaning as specified in that table. If this document is part of a set of documents, the same terms have the meaning as specified in such other documents. Conversely, the definition of these terms in such other documents does – for the purpose of this document – not affect their meaning as specified in the following table.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset</td>
<td>Anything that has a value to the organisation, like for instance information (e.g. databases, data files), software (e.g. system software, application software), physical assets (e.g. processors, tapes, power supply), services (e.g. computing services, heating, air-conditioning) and people (e.g. users, consultants).</td>
</tr>
<tr>
<td>Business transaction</td>
<td>All types settlement instructions, settlement restrictions and maintenance instructions as well as liquidity transfers processed by T2S.</td>
</tr>
<tr>
<td>Customer</td>
<td>Customer is defined as any entity that has a business relationship with the Eurosystem under the Framework Agreement or under the Currency Participation Agreement.</td>
</tr>
</tbody>
</table>
### Framework Agreement

**Schedule 10 – Annex 2 – Security requirements and controls**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| **Disaster [Major operational disruption]** | A high-impact disruption of normal business operations affecting a large metropolitan or geographic area and the adjacent communities that are economically integrated with it. In addition to impeding the normal operation of financial industry participants and other commercial organisations, major operational disruptions typically affect the physical infrastructure.  
Disasters (Major operational disruptions) can result from a wide range of events, such as earthquakes, hurricanes and other weather-related events, biological incidents (e.g. epidemics), terrorist attacks, and other intentional or accidental acts that cause widespread damage to the physical infrastructure. The most significant in terms of their impact are referred to as extreme events, which typically cause the destruction of, or severe damage to, physical infrastructure and facilities, the loss or inaccessibility of personnel, and restricted access to the affected area.  
[Taken from the BIS “High level principles for business continuity” published in August 2006] |
<p>| <strong>External Party</strong> | Any entity different from the Eurosystem (including the Central Banks it is composed of) and its Contractual Parties under the Framework Agreement or the Currency Participation Agreement |
| <strong>Impact</strong> | The result of an unwanted incident. |
| <strong>Impact analysis</strong> | The process of identifying the threats to the assets and the impact such threats could have, if the threat resulted in a genuine incident. Such analysis should quantify the value of the assets being protected to decide on the appropriate level of safeguards. |
| <strong>Information</strong> | The meaning that is currently assigned to data by means of the conventions applied to those data. |
| <strong>Information processing facilities</strong> | Any information processing system, service or infrastructure, or the physical locations housing them [ISO/IEC 27002:2005]. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security</td>
<td>Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved [ISO/IEC 27002:2005].</td>
</tr>
<tr>
<td>Information security event</td>
<td>An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [ISO/IEC TR 18044:2004].</td>
</tr>
<tr>
<td>Information security incident</td>
<td>An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC TR 18044:2004].</td>
</tr>
<tr>
<td>Inherent risk</td>
<td>The risk before risk treatment.</td>
</tr>
<tr>
<td>Policy</td>
<td>Overall intention and direction as formally expressed by management.</td>
</tr>
<tr>
<td>Recovery</td>
<td>Recovery (or recover) refers to the restoration of the processing service and settlement activities after a disruption including the processing of pending payment transactions.</td>
</tr>
<tr>
<td>Residual risk</td>
<td>The risk remaining after risk treatment.</td>
</tr>
<tr>
<td>Risk</td>
<td>Combination of the probability of an event and its consequence [ISO Guide 73:2002].</td>
</tr>
<tr>
<td></td>
<td>In other words, the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of or damage to the assets.</td>
</tr>
<tr>
<td>Risk analysis</td>
<td>Systematic use of information to identify sources and to estimate the risk [ISO Guide 73:2002].</td>
</tr>
<tr>
<td>Risk evaluation</td>
<td>The process of comparing the estimated risk against given risk criteria to determine the significance of the risk [ISO Guide 73:2002].</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Risk management</td>
<td>Coordinated activities to direct and control an organization with regard to risk. [ISO Guide 73:2002].</td>
</tr>
<tr>
<td></td>
<td><strong>Risk management</strong> is the ongoing process of <strong>risk assessment</strong> (evaluation of the impact or system criticality, and the likelihood of loss/damage occurring) leading to the definition of security requirements and the <strong>additional mitigation</strong> (by safeguards) <strong>and/or acceptance of remaining risks.</strong></td>
</tr>
<tr>
<td>Risk treatment</td>
<td>The process of selection and implementation of measures to modify risk [ISO Guide 73:2002].</td>
</tr>
<tr>
<td>Risk Profile</td>
<td>Having a different risk profile shall mean that the <em>alternate site</em> must be sufficiently remote from, and does not depend on the same <em>physical infrastructure</em> components as the primary business location. This minimises the risk that both could be affected by the same event. For example, the <em>alternate site</em> should be on a different power grid and central telecommunication circuit from the primary business location. [Derived from the BIS “High level principles for business continuity” published in August 2006]</td>
</tr>
<tr>
<td>Security assessment</td>
<td>A documented process reflecting the risk management procedure and presenting prevailing status of risks in relation to the security requirements, i.e. remaining risks for the security aspects such as: availability, integrity, confidentiality, authentication, authorisation, auditability and non-repudiation.</td>
</tr>
<tr>
<td>Security control</td>
<td>Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Security control is also used as a synonym for control, safeguard (measure), or countermeasure.</td>
</tr>
<tr>
<td>Security requirements</td>
<td>The types and levels of protection necessary to meet the security of the assets. The security requirements result from the security risks and are addressed by implementing suitable security controls.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security risk</td>
<td>The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of or damage to the assets.</td>
</tr>
<tr>
<td>Senior management</td>
<td>This is the highest decision making body of the service providing organisation (4CB).</td>
</tr>
<tr>
<td>Service</td>
<td>The term “Service” refers to all the T2S services as defined in the T2S Service Description document.</td>
</tr>
<tr>
<td>Service providing organisation</td>
<td>This term refers to all parts of the service provider’s (4CB) organisation that are involved in the T2S activities (design, build, test, operate, maintain, support T2S).</td>
</tr>
<tr>
<td>Service perimeter</td>
<td>This encompasses all infrastructural and technical components, business/organisational procedures and rules, human resources that are used to provide the T2S service.</td>
</tr>
<tr>
<td>Third party</td>
<td>A company or individual recognized as being independent of the Contractual Parties, and that provides services generally covered by a Service Level Agreement.</td>
</tr>
<tr>
<td>Threat</td>
<td>A potential cause of an unwanted incident, which may result in harm to a system or organization [ISO/IEC 13335-1:2004]</td>
</tr>
<tr>
<td>User</td>
<td>A user is an individual that can log into the service with a login name and requests or uses the services provided. As this document only applies to internal stakeholders (see T2S Information Security Policy), this term only refers to those users designing, building, testing (internal), operating (business and technical), maintaining and supporting (business and technical) T2S.</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>A weakness of an asset or group of assets that can be exploited by a threat [ISO/IEC 13335-1:2004]</td>
</tr>
</tbody>
</table>
### 2.2 Definitions

Specific values defined for T2S are listed in the following table:

<table>
<thead>
<tr>
<th>Value Name</th>
<th>Description</th>
<th>Value</th>
<th>Referencing Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Review Interval</td>
<td>The planned interval for reviewing the Information Security Policy.</td>
<td>Three years</td>
<td>4.1.2</td>
</tr>
<tr>
<td>Confidentiality Agreement Review Interval</td>
<td>The planned interval for reviewing confidentiality agreements.</td>
<td>Three years</td>
<td>5.1.4</td>
</tr>
<tr>
<td>Independent Security Review Interval</td>
<td>The planned interval for an independent review of the approach to managing information security and its implementation.</td>
<td>Three years</td>
<td>5.1.7</td>
</tr>
<tr>
<td>Physical Entry Controls Review Interval</td>
<td>The planned interval for reviewing physical entry controls.</td>
<td>Three months</td>
<td>8.1.2</td>
</tr>
<tr>
<td>Support Utilities Review Interval</td>
<td>The planned interval for reviewing support utilities.</td>
<td>Six months</td>
<td>8.2.2</td>
</tr>
<tr>
<td>Restoration Check Interval</td>
<td>The planned interval for checking the system restoration from backup.</td>
<td>One year</td>
<td>9.5.1</td>
</tr>
<tr>
<td>Distribution List Review Interval</td>
<td>The planned interval for the review of distribution list recipients.</td>
<td>Six months</td>
<td>9.7.3</td>
</tr>
<tr>
<td>Audit Logging Period</td>
<td>The period for keeping technical audit logs of the service.</td>
<td>Two years</td>
<td>9.10.1</td>
</tr>
<tr>
<td>Privileged Activities Review Interval</td>
<td>The planned interval for reviewing privileged activities on the service.</td>
<td>One business day</td>
<td>9.10.2</td>
</tr>
<tr>
<td>Administrator Log Review Interval</td>
<td>The planned interval for reviewing system administrator and operator logs.</td>
<td>One week</td>
<td>9.10.4</td>
</tr>
<tr>
<td>User Access Control Policy Review Interval</td>
<td>The planned interval for reviewing the User Access Control Policy.</td>
<td>Three years</td>
<td>10.1.1</td>
</tr>
</tbody>
</table>
## Framework Agreement

### Schedule 10 – Annex 2 – Security requirements and controls

<table>
<thead>
<tr>
<th>User Access Rights Review Interval</th>
<th>The planned interval for reviewing the user access rights.</th>
<th>Six months</th>
<th>10.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged User Access Rights Review Interval</td>
<td>The planned interval for reviewing the privileged user access rights.</td>
<td>Three months</td>
<td>10.2.4</td>
</tr>
<tr>
<td>Privileged Account Changes Logging Period</td>
<td>The period for keeping audit logs of changes to privileged accounts.</td>
<td>One year</td>
<td>10.2.4</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>The minimum length for user passwords.</td>
<td>Eight characters</td>
<td>10.3.1</td>
</tr>
<tr>
<td>Password Expiry Period</td>
<td>The expiry period for passwords after which a change is required.</td>
<td>Sixty days</td>
<td>10.3.1</td>
</tr>
<tr>
<td>Maximum Logon Attempts</td>
<td>The maximum number of failed logon attempts for a user before the account is disabled.</td>
<td>Three attempts</td>
<td>10.3.1</td>
</tr>
<tr>
<td>Remote Connections Idle Interval</td>
<td>The idle time after which a re-authentication of a remotely connected user is required.</td>
<td>10 minutes</td>
<td>10.4.2</td>
</tr>
<tr>
<td>Period for Keeping Previous Passwords</td>
<td>The period to keep previously used passwords to prevent reuse.</td>
<td>One year</td>
<td>10.5.3</td>
</tr>
<tr>
<td>Session Time-out</td>
<td>The period of inactivity before a user session is closed.</td>
<td>15 minutes</td>
<td>10.5.5</td>
</tr>
<tr>
<td>Information Access Restriction Review Interval</td>
<td>The planned interval for the review of the service’s output to remove redundant information.</td>
<td>Three years</td>
<td>10.6.1</td>
</tr>
<tr>
<td>Business Continuity Test Interval</td>
<td>The planned interval for testing business continuity.</td>
<td>Six months</td>
<td>13.1.5</td>
</tr>
<tr>
<td>Business Continuity Review Interval</td>
<td>The planned interval for reviewing the business continuity plan.</td>
<td>Six months</td>
<td>13.1.5</td>
</tr>
<tr>
<td>Compliance Review Interval</td>
<td>The planned interval for a full compliance review of the service with security policies and requirements.</td>
<td>Three years</td>
<td>14.2.1</td>
</tr>
</tbody>
</table>
3 Structure of the security requirements and controls

The document consists of 11 Information Security Management Domains which mainly serve the purpose of structuring the broad field of information security. On a second layer the Security Requirements specifying the objectives that should be achieved are defined. Finally on a third layer the (benchmark) Security Controls are specified.

Exhibit 2: Structure of the security requirements and controls

The eleven information security management domains are listed in the following (the number in brackets indicates the number of main security requirements included within each clause):

a) Security Policy (1) – see chapter 4;

b) Organising Information Security (2) – see chapter 5;

c) Asset Management (2) – see chapter 6;

d) Human Resources Security (3) – see chapter 7;
e) Physical and Environmental Security (2) – see chapter 8;
f) Communications and Operations Management (10) – see chapter 9;
g) Access Control (7) – see chapter 10;
h) Information Systems Acquisition, Development and Maintenance (6) – see chapter 11;
i) Information Security Incident Management (2) – see chapter 12;
j) Business Continuity Management (1) – see chapter 13;
k) Compliance (3) – see chapter 14.

Note: The order of the clauses does not imply their importance.

Under each information security management domain the security requirements are specified. Each requirement section contains:

a) a control objective stating what is to be achieved, i.e. the actual security requirement; and
b) one or more security controls that should be implemented to meet the security requirements.

The security controls are the processes and measures that should be implemented within the service perimeter to meet the security requirements.

4 Security policy

4.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

4.1.1 Information security policy document

Control: An information security policy document² must be approved, by senior management published and communicated to all relevant parties (including users and external parties).

² This refers to a specific information security policy defined by the Service providing organisation
The senior management must be named in the information security policy document. The policy document must state the commitment to information security and set out the approach to managing information security. It must contain statements concerning:

1. a definition of information security, its overall objectives and scope and the importance of information security;
2. a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
3. a framework for setting control objectives and controls, including the structure of risk assessment and risk management;
4. a brief explanation of the security policies, principles, and compliance requirements including:
   1) compliance with legislative, regulatory, and contractual requirements;
   2) security education, training, and awareness requirements;
   3) business continuity management;
   4) consequences of information security policy violations;
5. a definition of responsibilities for information security management, including reporting information security incidents;
6. references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules that users should comply with.

This information security policy must be communicated to all users in a form that is accessible and understandable to the intended reader.

4.1.2 Review of the information security policy

Control: The information security policy must be reviewed at planned intervals and/or when significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

The information security policy must have an owner who has approved management responsibility for the development, review, and evaluation of the information security policy.

The review of the information security policy must take account of the results of other management processes, like for instance change and incident management. The information security policy must be reviewed at planned intervals (Policy Review Interval) and/or when significant changes occur.
The input to the review of the information security policy should include information on:

a) feedback from interested parties;
b) results of independent reviews;
c) status of preventive and corrective actions;
d) results of previous management reviews;

e) process performance and information security policy compliance;
f) changes that could affect the approach to managing information security, including changes to the organisational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment;

g) trends related to threats and vulnerabilities;
h) reported information security incidents;
i) recommendations provided by relevant authorities.

The output from the review must include any decisions and actions related to:

a) improvement of the approach to managing information security and its processes;
b) improvement of control objectives and controls;
c) improvement in the allocation of resources and/or responsibilities.

A record of the review must be maintained.

The approval for the revised policy must be obtained from the senior management.

5 Organising information security

5.1 Internal organisation

Objective: To manage information security effectively.

A management framework must be established to initiate and control the implementation of information security.

The senior management must approve the information security policy, assign security roles and co-ordinate and review the implementation of security.
5.1.1 Management commitment to information security

Control: The senior management must actively and visibly support security through clear direction, demonstrated commitment, explicit assignment of roles and responsibilities, and acknowledgment of information security responsibilities.

The senior management must:

a) ensure that information security goals are identified, meet the organisational requirements, and are integrated in relevant processes;

b) formulate, review, and approve an information security policy;

c) review the effectiveness of the implementation of the information security policy;

d) provide clear direction and visible management support for security initiatives;

e) provide the resources needed for information security;

f) approve assignment of specific roles and responsibilities for information security;

g) initiate plans and programs to maintain information security awareness;

h) ensure that the implementation of information security controls is co-ordinated.

The needs for internal or external specialist information security advice must be identified, and results of the advice must be reviewed and coordinated throughout the service perimeter.

5.1.2 Information security co-ordination

Control: Information security activities must be co-ordinated by representatives from different parts within the service perimeter with relevant roles and job functions.

Typically, information security co-ordination should involve the cooperation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management.

This activity must:

a) ensure that security activities are executed in compliance with the information security policy;

b) identify how to handle non-compliances;

c) approve methodologies and processes for information security, e.g. risk assessment, information classification;

d) identify significant threat changes and exposure of information and information processing facilities to threats;
e) assess the adequacy and co-ordinate the implementation of information security controls;

f) effectively promote information security education, training and awareness;

g) evaluate information received from the monitoring and reviewing of information security incidents, and recommend actions in response to identified information security incidents.

5.1.3 Allocation of information security responsibilities

Control: All information security responsibilities must be clearly defined.

Allocation of information security responsibilities must be done in accordance with the information security policy (see clause 4). Responsibilities for the protection of individual assets and for carrying out specific security processes must be clearly identified. This responsibility must be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities.

The senior management may delegate security tasks to others. Nevertheless senior management remains responsible and must determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible must be clearly stated; in particular the following must take place:

a) the assets and security processes associated with each particular system must be identified and clearly defined;

b) the entity responsible for each asset or security process must be assigned and the details of this responsibility must be documented;

c) authorisation levels must be clearly defined and documented.

The allocation of roles and responsibilities in the risk management process are described in the risk management manual.

5.1.4 Confidentiality agreements

Control: Requirements for confidentiality or non-disclosure agreements for the protection of information must be identified and regularly reviewed at planned intervals.

Confidentiality or non-disclosure agreements must address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or non-disclosure agreements, the following elements must be implemented:

a) a definition of the information to be protected (e.g. confidential information);
b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

c) required actions when an agreement is terminated;

d) responsibilities and actions of signatories to avoid unauthorised information disclosure (such as ‘need to know’);

e) ownership of information and intellectual property, and how this relates to the protection of confidential information;

f) the permitted use of confidential information, and rights of the signatory to use information;

g) the right to audit and monitor activities that involve confidential information;

h) process for notification and reporting of unauthorised disclosure or confidential information breaches;

i) terms for information to be returned or destroyed at agreement cessation; and

j) expected actions to be taken in case of a breach of this agreement.

Confidentiality and non-disclosure agreements must comply with all applicable laws and regulations for the jurisdiction to which it applies.

Requirements for confidentiality and non-disclosure agreements must be regularly reviewed at planned intervals (Confidentiality Agreement Review Interval) and/or when changes occur that influence these requirements.

5.1.5 Contact with authorities

Control: Contacts with relevant authorities must be maintained.

Procedures must be in place that specify who (e.g. law enforcement, fire department, supervisory authorities) and when and by whom authorities should be contacted. Procedures must also be in place depicting how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken.

5.1.6 Contact with special interest groups

Control: Contacts with special interest groups or other specialist security forums and professional associations must be maintained in order to ensure that:

a) knowledge about best practices is improved and to stay up to date with relevant security information;
b) the understanding of the information security environment is current and complete;

c) early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities are received;

d) access to specialist information security advice is gained;

e) information about new technologies, products, threats, or vulnerabilities is shared and exchanged;

f) suitable liaison points when dealing with information security incidents are provided.

5.1.7 Independent review of information security

Control: The approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) must be reviewed independently by recognised experts at planned intervals, and/or when significant changes to the security implementation occur.

Such an independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness to managing information security.

Information security review activities are carried out at planned intervals (Independent Security Review Interval) and/or when significant changes to the security implementation occur by individuals independent of the area under review, e.g. the T2S Board, internal audit function, an independent manager or a third party organisation specialising in such reviews. Individuals carrying out these reviews must have the appropriate skills and experience.

The results of the independent review are recorded and reported to the T2S Board. These records must be maintained.

If the independent review identifies that the approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document, the senior management will be informed and should consider corrective actions.

5.1.8 Authorisation process for information processing facilities

Control: A management authorisation process shall be defined and implemented.

---

3 This independent review is usually triggered by the Level 2 Governance.
This control is not applicable for the time being, as all changes are covered by the change management process.

5.2 External parties

Objective: To maintain the security of the service’s information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

The security of the service’s information and information processing facilities must not be reduced by the introduction of external party products or services.

Any access to the service’s information processing facilities and processing and communication of information by external parties must be controlled. Where there is a business need for working with external parties that may require access to the service’s information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment must be carried out to determine security implications and control requirements. Controls must be agreed and defined in an agreement with the external party.

5.2.1 Identification of risks related to external parties

Control: The risks to the service’s information and information processing facilities from business processes involving external parties must be identified and controls implemented before granting access.

Where there is a need to allow an external party access to the information processing facilities or information, a risk assessment must be carried out to identify any requirements for specific controls. The identification of risks related to external party access must take into account the following issues:

a) the information processing facilities an external party is required to access;

b) the type of access the external party will have to the information and information processing facilities, e.g.:

1) physical access, e.g. to offices, computer rooms, filing cabinets;

2) logical access, e.g. to databases, information systems;

3) network connectivity between the service and the external party’s network(s), e.g. permanent connection, remote access;

4) whether the access is taking place on-site or off-site;
c) the value and the classification level of the information involved, and its criticality for business operations;

d) the controls necessary to protect information that is not intended to be accessible by external parties;

e) the external party personnel involved in handling the service’s information;

f) how the personnel authorised to have access can be identified, the authorisation verified, and how often this needs to be reconfirmed;

g) the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;

h) the impact of access not being available to the external party when required, and the impact of the external party entering or receiving inaccurate or misleading information;

i) practices and procedures dealing with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;

j) legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account.

Access by external parties to the service’s information must not be provided until the controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party.

It must be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the service’s information and information processing facilities.

The controls 5.2.2 and 5.2.3 cover different external party arrangements, e.g. including:

a) service providers, such as ISPs, network providers, telephone services, maintenance and support services;

b) managed security services;

c) customers;

d) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call centre operations;
5.2.2 Addressing security when dealing with the customer

Control: All identified security requirements must be addressed using a defined process with documented results, before giving customers access to the service’s information or assets. The following terms must be implemented to address security prior to giving customers access to any of the assets (depending on the type and extent of access given, not all of them might apply):

a) the product or service to be provided;

b) a description of each service to be made available;

c) the target level of service and unacceptable levels of service;

d) the respective liabilities of the service providing organisation and the customer;

e) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries.

5.2.3 Addressing security in third party agreements

Control: Agreements with third parties involving accessing, processing, communicating or managing the service’s information or information processing facilities, or adding products or services to information processing facilities must cover all relevant security requirements. The following terms should be included in the agreement in order to satisfy the identified security requirements:

a) The information security policy;

b) controls to ensure asset protection, including:

1. procedures to protect assets, including information, software and hardware;

2. any required physical protection controls and mechanisms;

3. controls to ensure protection against malicious software;
4. procedures to determine whether any compromise of the assets, e.g. loss or
modification of information, software and hardware, has occurred;

5. controls to ensure the return or destruction of information and assets at the end
of, or at an agreed point in time during, the agreement;

6. confidentiality, integrity, availability, and any other property of the assets;

7. restrictions on copying and disclosing information, and using confidentiality
agreements;

c) user training in methods, procedures, and security;

d) ensuring user awareness for information security responsibilities and issues;

e) provision for the transfer of personnel, where appropriate;

f) responsibilities regarding hardware and software installation and maintenance;

g) a clear reporting structure and agreed reporting formats;

h) a clear and specified process of change management;

i) access control policy, covering:

1. the different reasons, requirements, and benefits that make the access by the third
   party necessary;

2. permitted access methods, and the control and use of identifiers such as user IDs
   and passwords;

3. an authorisation process for user access and privileges;

4. a requirement to maintain a list of individuals authorised to use the services
   being made available, and what their rights and privileges are with respect to
   such use;

5. a statement that all access that is not explicitly authorised is forbidden;

6. a process for revoking access rights or interrupting the connection between
   systems;

j) arrangements for reporting, notification, and investigation of information security
   incidents and security breaches, as well as violations of the requirements stated in the
   agreement;

k) a description of the product or service to be provided, and a description of the
   information to be made available along with its security classification;
l) the target level of service and unacceptable levels of service;
m) the definition of verifiable performance criteria, their monitoring and reporting;
n) the right to monitor, and revoke, any activity related to the assets;
o) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
p) the establishment of an escalation process for problem resolution;
q) service continuity requirements, including measures for availability and reliability, in accordance with business priorities;
r) the respective liabilities of the parties to the agreement;
s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organisations in other countries;
t) intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work;
u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;
v) conditions for renegotiation/termination of agreements:

1. a contingency plan must be in place in case either party wishes to terminate the relation before the end of the agreements;
2. renegotiation of agreements if the security requirements change;
3. change of current documentation of asset lists, licences, agreements or rights relating to them.
6 Asset management

6.1 Responsibility for assets

Objective: To achieve and maintain protection of assets.

All assets must be accounted for and have a nominated owner.

Owners must be identified for all assets and the responsibility for the maintenance of controls must be assigned. The implementation of specific controls may be delegated by the asset owner as appropriate but the owner remains responsible for the proper protection of the assets.

6.1.1 Inventory of assets

Control: All assets must be clearly identified and an inventory of all important (its business value and its security classification) assets drawn up and maintained. Regular audits of the asset inventory must be performed.

All assets must be identified and the importance of these assets must be documented. The asset inventory must include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.

However, in order to reduce the work associated with drawing up the inventory grouping of assets is allowed. Criteria for grouping are:

a) similar assets;

b) similar security requirements;

c) assets are used in the same process and protection requirements are valid throughout;

d) assets can be considered as a unit.

Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets must be identified and documented.

There are many types of assets, including:

a) information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
b) software assets: application software, system software, development tools, and utilities;

c) physical assets: computer equipment, communications equipment, removable media, and other equipment;

d) services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;

e) people, and their qualifications, skills, and experience.

6.1.2 Ownership of assets

Control: All information and assets associated with information processing facilities must have for security purposes a designated asset owner.

The asset owner is responsible for:

a) ensuring that information and assets associated with information processing facilities are classified;

b) defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

6.1.3 Acceptable use of assets

Control: Rules for the acceptable use of information and assets associated with information processing facilities must be identified, documented, and implemented.

All employees, contractors and third party users must follow rules for the acceptable use of information and assets associated with information processing facilities, including:

a) rules for electronic mail and Internet usages;

b) guidelines for the use of mobile devices, especially for the use outside the premises;

Specific rules or guidance must be provided by the senior management. Employees, contractors and third party users using or having access to assets must be aware of the limits existing for their use of the information and assets associated with information processing facilities, and resources. They must be responsible for their use of any information processing resources and of any use carried out under their responsibility.

---

The term ‘asset owner’ identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term ‘owner’ does not mean that the person actually has any property rights to the asset.
6.2 Information classification

Objective: To ensure that information receives an appropriate level of protection.

Information must be classified to indicate the need, priorities, and expected degree of protection when handling the information.

6.2.1 Classification guidelines

Control: Information must be classified in terms of criticality, value and sensitivity (level of confidentiality) taking legal requirements into account as well.

Classifications and associated protective controls for information must take account of business needs for sharing or restricting information and the business impacts associated with such needs.

Classification guidelines must include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy.

6.2.2 Information labelling and handling

Control: A set of procedures for information labelling and handling must be developed and implemented in accordance with the classification scheme adopted by the service.

Procedures for information labelling need to cover information assets in physical and electronic formats.

Output from systems containing information that is classified as being sensitive or critical must carry a classification label (in the output). The labelling must reflect the classification according to the rules established in 6.2.1.

For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction must be defined. This should also include the procedures for chain of custody and logging of any security event.

Agreements with other organisations that include information sharing must include procedures to identify the classification of that information and to interpret the classification labels from other organisations.

---

5 The ECB classification scheme should be used as reference document as long as a common ESCB scheme is not deployed.
7 Human resources security

7.1 Prior to employment

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles for which they are considered, and to reduce the risk of theft, fraud or misuse of facilities.

7.1.1 Roles and responsibilities

Control: Security roles and responsibilities of employees, contractors and third party users must be defined and documented in accordance with the information security policy.

Security roles and responsibilities must include the requirement to:

a) implement and act in accordance with the information security policies;

b) protect assets from unauthorised access, disclosure, modification, destruction or interference;

c) execute particular security processes or activities;

d) ensure responsibility is assigned to the individual for actions taken;

e) report security events, potential events or security risks.

Security roles and responsibilities must be defined and clearly communicated to job candidates during the pre-employment process.

7.1.2 Screening

Control: Background verification checks on all candidates for employment, contractors, and third party users must be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

Verification checks must take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:

a) availability of satisfactory character references, e.g. one business and one personal;

---

6 Explanation: The word ‘employment’ is meant here to cover all of the following different situations: employment of people, appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.
b) a check (for completeness and accuracy) of the applicant’s curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity check (passport or similar document);

e) more detailed checks, such as credit checks or checks of criminal records.

Procedures must define criteria and limitations for verification checks, e.g. who is eligible to
screen people, and how, when and why verification checks are carried out.

A screening process must also be carried out for contractors, and third party users. Where
contractors are provided through an agency the contract with the agency must clearly specify the
agency’s responsibilities for screening and the notification procedures they need to follow if
screening has not been completed or if the results give cause for doubt or concern. In the same
way, the agreement with the third party must clearly specify all responsibilities and notification
procedures for screening.

Information on all candidates being considered for positions within the organisation must be
collected and handled in accordance with any applicable legislation existing in the relevant
jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand
about the screening activities.

7.1.3 Terms and conditions of employment

Control: As part of their contractual obligation, employees, contractors and third party users must
agree and sign the terms and conditions of their employment contract, which must state the
responsibilities of both sides concerning information security. Terms and conditions must be in
accordance with any applicable legislation existing in the relevant jurisdiction.

The terms and conditions of employment must reflect the security policy in addition to clarifying
and stating:

a) that all employees, contractors and third party users who are given access to sensitive
information must sign a confidentiality or non-disclosure agreement prior to being given
access to information processing facilities;

b) the employee’s, contractor’s and third party user’s legal responsibilities and rights, e.g.
regarding copyright laws, data protection legislation;

c) responsibilities for the classification of information and management of assets associated
with information systems and services handled by the employee, contractor or third party
user;
d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;

e) responsibilities for the handling of personal information, including personal information created as a result of, or in the course of, employment with the respective central bank;

f) responsibilities that are extended outside the hosting premises and outside normal working hours, e.g. in the case of home-working;

g) actions to be taken if the employee, contractor or third party user disregards the security requirements.

It must be ensured that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment.

7.2 During employment

Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support the information security policy in the course of their normal work, and to reduce the risk of human error.

7.2.1 Management responsibilities

Control: Management must require employees, contractors and third party users to apply security in accordance with established policies and procedures of the service providing organisation.

Management responsibilities must include ensuring that employees, contractors and third party users:

a) are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information;

b) are provided with guidelines to state security expectations of their role;

c) are motivated to fulfil the security policies set-up by the senior management;

d) achieve a level of awareness on security relevant to their roles and responsibilities;

e) conform to the terms and conditions of employment, which includes the information security policy and appropriate methods of working;
7.2.2 Information security awareness, education, and training

**Control:** All employees, contractors and third party users must receive appropriate awareness training and regular updates on the policies and procedures, as relevant for their job function. Awareness training must commence with a formal induction process designed to introduce the information security policy, procedures and expectations before access to information or services is granted.

Ongoing training must include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process.

7.2.3 Disciplinary process

**Control:** There must be a formal disciplinary process in accordance with any applicable legislation existing in the relevant jurisdiction for employees who have committed a security breach. The disciplinary process must not commence without prior verification that a security breach has occurred.

7.3 Termination or change of employment

**Objective:** To ensure that employees, contractors and third party users exit or change employment in an orderly manner (as defined in the following control sections).

7.3.1 Termination responsibilities

**Control:** Responsibilities for performing employment termination or change of employment must be clearly defined and assigned. The communication of termination responsibilities must include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement, and the terms and conditions of employment continuing for a defined period after the end of the employee’s, contractor’s or third party user’s employment.

---

7 Appropriate contractual remedies against contractors and third-party users who have committed a security breach are covered as part of the third party agreements as described in chapter 5.2.3.
Responsibilities and duties still valid after termination of employment must be contained in employee’s, contractor’s or third party user’s contracts.

Changes of responsibility or employment must be managed as the termination of the respective responsibility or employment, and the new responsibility or employment must be controlled as described in clause 7.1.

### 7.3.2 Return of assets

**Control:** All employees, contractors and third party users must return all assets in their possession upon termination of their employment, contract or agreement.

The termination process must be formalised to include the return of all previously issued software, corporate documents, and equipment. Other assets such as mobile computing devices, access cards, software, manuals, and information stored on electronic media also need to be returned.

In cases where an employee, contractor or third party user purchases equipment or uses their own personal equipment, procedures must be followed to ensure that all relevant information is returned and securely erased from the equipment.

In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information must be documented and transferred to the appointed people.

### 7.3.3 Removal of access rights

**Control:** The access rights of all employees, contractors and third party users to information and information processing facilities must be removed upon termination of their employment, contract or agreement or adjusted upon change.

Changes of an employment must be reflected in removal of all access rights that were not approved for the new employment. The access rights that must be removed or adapted include physical and logical access, keys, identification cards, information processing facilities, subscriptions, and removal from any documentation that identifies them as a current member of the respective central bank. If a departing employee, contractor or third party user has known passwords for accounts remaining active, these must be changed upon termination or change of employment, contract or agreement.

Access rights for information assets and information processing facilities must be reduced or removed at the time the employment terminates or changes.
8  Physical and environmental security

8.1  Secure areas

Objective: To prevent unauthorised physical access, damage, and interference to the hosting premises and information.

Critical or sensitive information processing facilities must be housed in secure areas, protected by defined security perimeters, with security barriers and entry controls. They must be physically protected from unauthorised access, damage, and interference.

The protection provided must be commensurate with the identified risks.

8.1.1  Physical security perimeter

Control: Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) must be used to protect areas that contain the service’s information and information processing facilities.

The following must be implemented for physical security perimeters:

a) security perimeters must be clearly defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b) perimeters of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors must be suitably protected against unauthorised access with control mechanisms, e.g. bars, alarms, locks etc; doors and windows should be locked when unattended and external protection should be implemented for windows;

c) a manned reception area or other means to control physical access to the site or building must be in place;

d) access to sites and buildings must be restricted to authorised personnel only;

e) physical barriers should, where applicable, be built to prevent unauthorised physical access and environmental contamination;

f) all fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to
suitable regional, national, and international standards; they must operate in accordance
with local fire code in a failsafe manner;

g) intruder detection systems must be installed to national, regional or international
standards and tested (at least once a year) to cover all external doors and accessible
windows; unoccupied areas should be alarmed at all times; cover should also be provided
for other areas, e.g. computer room or communications rooms;

h) information processing facilities managed by the service providing organisation should
be physically separated⁸ from those managed by third parties.

8.1.2 Physical entry controls

Control: Secure areas must be protected by entry controls to ensure that only authorised
personnel are allowed access.

The following must be implemented:

a) the date and time of entry and departure of visitors must be recorded;

b) visitors must be supervised unless their access has been previously approved; they must
only be granted access for specific, authorised purposes and must be provided with
instructions on the security requirements of the area and on emergency procedures;

c) access to the areas (e.g. computer rooms and office rooms) must be controlled and
restricted to authorised persons only; authentication controls, e.g. access control card plus
PIN, must be used to authorise and validate all access;

d) an audit trail of all access must be maintained (see 14.1.3);

e) all employees, contractors, third party users and visitors must be required to wear some
form of visible identification and must immediately notify security personnel if they
encounter unescorted visitors not wearing visible identification;

f) third party support service personnel must be granted restricted access to secure areas
only when required; this access must be authorised and monitored;

g) access rights to secure areas must be reviewed at planned intervals (Physical Entry

Controls Review Interval) and updated, and revoked when necessary.

⁸ Physical separation in this context is not required if third party support personnel is always supervised by internal
staff.
8.1.3  Securing offices, rooms, and facilities

Control: Physical security for offices, rooms, and facilities must be designed and applied.

The following must be implemented to secure offices, rooms, and facilities:

a) account must be taken of relevant health and safety regulations and standards;

b) key facilities must be sited to avoid access by the public;

c) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;

d) directories and internal telephone books identifying locations of sensitive information processing facilities must not be readily accessible by the public.

8.1.4  Protecting against external and environmental threats

Control: Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster must be designed and applied.

Consideration must be given to any security threats presented by neighbouring premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street.

The following guidelines must be implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a) hazardous or combustible materials must not be stored within a secure area;

b) bulk supplies such as stationery must not be stored within a secure area;

c) fallback equipment and back-up media must be sited at a secondary site with a different risk profile to avoid damage from a disaster affecting the main site;

d) fire fighting equipment must be provided and suitably placed.

8.1.5  Working in secure areas

Control: Physical protection and guidelines for working in secure areas must be designed and applied.
The following must be implemented:

a) personnel must only be aware of the existence of, or activities within, a secure area on a need to know basis;

b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

c) vacant secure areas (i.e. rooms containing critical components but not permanently staffed) must be physically locked and periodically checked;

d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorised.

8.1.6 Public access, delivery, and loading areas

Control: Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises must be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

The following must be implemented:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorised personnel;

b) the delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;

c) the external doors of a delivery and loading area must be secured when the internal doors are opened;

d) incoming material should be inspected for potential threats before this material is moved from the delivery and loading area to the point of use;

e) incoming material should be registered in accordance with asset management procedures on entry to the site.

8.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the service providing organisation’s activities.

Equipment must be protected from physical and environmental threats.
8.2.1 Equipment sitting and protection

Control: Equipment must be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

The following must be implemented to protect equipment:

a) equipment must be sited to minimise unnecessary access into work areas;

b) information processing facilities handling sensitive data must be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorised persons during their use, and storage facilities secured to avoid unauthorised access;

c) items requiring special protection must be isolated to reduce the general level of protection required;

d) controls must be adopted to minimise the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;

e) environmental conditions, such as temperature and humidity, must be monitored for conditions, which could adversely affect the operation of information processing facilities;

f) lightning protection must be applied to all buildings and lightning protection filters must be fitted to all incoming power and communications lines.

8.2.2 Supporting utilities

Control: Equipment must be protected from power failures and other disruptions caused by failures in supporting utilities.

All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning must be adequate for the systems they are supporting. At regular intervals (Support Utilities Review Interval) the support utilities must be inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. An electrical supply must be provided that conforms to the equipment manufacturer’s specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running must be in place for equipment supporting critical business operations. Power contingency plans must cover the action to be taken on failure of the UPS. A back-up generator must be in place if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel must be available to ensure that the generator can perform for a prolonged period.
equipment and generators must be checked at least twice a year to ensure it has adequate capacity
and tested in accordance with the manufacturer’s recommendations. In addition, consideration
should be given to using multiple power sources or, if the site is large a separate power
substation.

Emergency power off switches must be located near emergency exits in equipment rooms to
facilitate rapid power down in case of an emergency. Emergency lighting must be provided in
case of main power failure.

The water supply must be stable and adequate to supply air conditioning, humidification
equipment and fire suppression systems (where used).

Malfunctions in the water supply system may damage equipment or prevent fire suppression
from acting effectively. Therefore an alarm system to detect malfunctions in the supporting
utilities must be installed.

Telecommunications equipment must be connected to the utility provider by at least two diverse
routes to prevent failure in one connection path removing voice services. Voice services must be
adequate to meet local legal requirements for emergency communications.

**8.2.3  Cabling security**

**Control:** Power and telecommunications cabling carrying data or supporting information services
must be protected from interception or damage.

The following must be implemented:

a) power and telecommunications lines into information processing facilities must be
underground, where possible, or subject to adequate alternative protection;

b) network cabling must be protected from unauthorised interception or damage, for
example by using a conduit or by avoiding routes through public areas;

c) power cables should be segregated from communications cables to prevent interference;

d) clearly identifiable cable and equipment markings should be used to minimise handling
errors, such as accidentally patching of wrong network cables;

e) a documented patch list should be used to reduce the possibility of errors;

f) installation of armoured conduit and locked rooms or boxes at inspection and termination
points;

g) use of alternative routings and/or transmission media providing security;

h) controlled access to patch panels and cable rooms.
8.2.4 Equipment maintenance

Control: Equipment must be correctly maintained to ensure its continued availability and integrity.

The following must be implemented:

a) equipment must be maintained in accordance with the supplier’s recommended service intervals and specifications;

b) only authorised maintenance personnel must carry out repairs and service equipment;

c) records must be kept of all suspected or actual faults, and all preventive and corrective maintenance;

d) all requirements imposed by insurance policies must be complied with.

8.2.5 Security of equipment off-premises

Control: Security must be applied to off-site equipment taking into account the risks of it being outside of the hosting premises.

Regardless of ownership, the use of any information processing equipment outside the hosting premises must be authorised by responsible management.

The following guidelines must be implemented for the protection of off-site equipment:

a) equipment and media\(^9\) taken off the hosting premises must not be left unattended in public places;

b) portable computers should be carried as hand luggage;

c) manufacturers’ instructions for protecting equipment must be observed at all times, e.g. protection against exposure to strong electromagnetic fields;

d) home-working controls must be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office;

e) adequate insurance cover must be in place to protect equipment off-site.

---

\(^9\) Information storing and processing equipment includes all forms of personal computers, organisers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location
8.2.6 Secure disposal or re-use of equipment

Control: All items of equipment containing storage media must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Devices containing sensitive information must be physically destroyed or the information must be destroyed, deleted or securely overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.

8.2.7 Removal of property

Control: Equipment, information or software must not be taken off-site without prior authorisation.

The following guidelines must be implemented:

a) equipment, information or software must not be taken off-site without prior authorisation;

b) employees, contractors and third party users who have authority to permit off-site removal of assets must be clearly identified;

c) time limits for equipment removal should be set and returns checked for compliance;

d) equipment must be recorded as being removed off-site and recorded when returned to the issuing department.

9 Communications and operations management

9.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operation of all information processing facilities must be established. This includes the development of operating procedures.

Segregation of duties must be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.
9.1.1 Documented operating procedures

Control: Operating procedures must be documented, maintained, and made available to all users who need them.

Documented procedures must be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures must specify the instructions for the detailed execution of each job including:

a) processing and handling of information;

b) backup (see 9.5);

c) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

d) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities;

e) support contacts in the event of unexpected operational or technical difficulties;

f) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs;

g) system restart and recovery procedures for use in the event of system failure;

h) the management of audit-trail and system log information (see 9.10).

Operating procedures, and the documented procedures for system activities, must be treated as formal documents and changes authorised by management as part of the change management process.

9.1.2 Change management

To avoid redundancies this control has been merged with control 11.5.1.

9.1.3 Segregation of duties

Control: Duties and areas of responsibility must be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of assets.
Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care must be taken that no single person can access, modify or use assets without authorisation or detection. The initiation of an event should be separated from its authorisation for example by implementing the four-eye principle. Controls must be designed and implemented with consideration of fraud scenario including the possible collusion of several players.

The initiation of an event must be separated from its authorisation meaning segregation of activities which require collusion in order to defraud (critical business functions), i.e. features must be in place in order to ensure that no person is in a position to alter sensitive business data single-handed, e.g. dispatching of a payment.

9.1.4 Separation of development, test, and operational facilities

**Control:** Development, test, and operational facilities must be separated to reduce the risks of unauthorised access or changes to the operational system.

The following must be implemented:

a) rules for the transfer of software from development to operational status must be defined and documented;

b) development and operational software must run on different systems or computer processors and in different domains or directories;

c) compilers, editors, and other development tools or system utilities should not be accessible from operational systems when not required;

d) the test system environment should emulate the operational system environment as closely as possible;

e) users should use different user profiles for operational and test systems;

f) menus should display identification messages to reduce the risk of error;

g) sensitive data should not be copied into the test system environment (see 11.4.2).

9.2 Third Party service delivery management

**Objective:** To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The senior management must check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.
9.2.1 Service delivery

Control: It must be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Service delivery by a third party must include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the senior management must plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and must ensure that security is maintained throughout the transition period.

The senior management must ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

9.2.2 Monitoring and review of third party services

Control: The services, reports and records provided by the third party must be regularly monitored and reviewed, and audits (where applicable) must be carried out regularly.

Monitoring and review of third party services must involve a service management relationship and process between the service providing organisation and the third party to:

a) monitor service performance levels to check adherence to the agreements;

b) review service reports produced by the third party and arrange regular progress meetings as required by the agreements;

c) receive information about information security incidents and review of this information conducted jointly;

d) review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

e) resolve and manage any identified problems.

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, it should be ensured that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources must be made available to monitor the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action must be taken when deficiencies in the service delivery are observed.
9.2.3 Managing changes to third party services

Control: Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, must be managed, taking into account the criticality of business systems and processes involved after a thorough re-assessment of risks.

The process of managing changes to a third party service must include rules for:

a) changes requested by the service providing organisation impacting the third party:
   1. enhancements to the current service offered;
   2. development of any new applications and systems;
   3. modifications or updates of policies and procedures;
   4. new controls to resolve information security incidents and to improve security.

b) changes in the third party services that impact the service providing organisation:
   1. changes and enhancement to networks;
   2. use of new technologies;
   3. adoption of new products or newer versions/releases;
   4. new development tools and environments;
   5. changes to physical location of service facilities;
   6. change of vendors.

9.3 System planning and acceptance

Objective: To minimise the risk of systems failures.

Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance. Projections of future capacity requirements must be made, to reduce the risk of system overload. The operational requirements of new systems must be established, documented, and tested prior to their acceptance and use.

9.3.1 Capacity management

Control: The use of resources must be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

For each new and ongoing activity, capacity requirements must be identified. System tuning and monitoring must be applied to ensure and, where necessary, improve the availability and
efficiency of systems. Detective controls must be put in place to indicate problems in due time.

Projections of future capacity requirements must take account of new business and system requirements and current and projected trends in the information processing capabilities.

Particular attention needs to be paid to any key resources in order to avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

9.3.2 System acceptance

Control: Acceptance criteria for new information systems, upgrades, and new versions must be established, and suitable tests of the system(s) carried out during development and prior to acceptance.

It must be ensured that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions must only be migrated into production after obtaining formal acceptance. The following must be established prior to formal acceptance being provided:

a) performance and computer capacity requirements;

b) error recovery and restart procedures, and contingency plans;

c) preparation and testing of routine operating procedures;

d) agreed set of security controls in place;

e) effective manual procedures;

f) business continuity arrangements;

g) evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;

h) evidence that consideration has been given to the effect the new system has on the overall security of the service;

i) training in the operation or use of new systems;

j) ease of use, as this affects user performance and avoids human error.

Tests involving the operations function and users must be carried out to confirm that all acceptance criteria have been fully satisfied. Testing activities and results must be properly documented.
9.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Precautions are required to prevent and detect the introduction of malicious code and unauthorised mobile code.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users must be made aware of the dangers of malicious code.

9.4.1 Controls against malicious code

Control: Detection, prevention, and recovery controls to protect against malicious code and user awareness procedures must be implemented.

Protection against malicious code must be based on malicious code detection and repair software, security awareness, system access and change management controls. The following must be implemented:

a) establishing a formal policy prohibiting the use of unauthorised software;

b) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken;

c) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorised amendments should be formally investigated (optional);

d) installation and maintenance of up-to-date malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out must include:

1. checking any files on electronic or optical media, and files received over networks, for malicious code before use;

2. checking electronic mail attachments and downloads for malicious code before use; this check must be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the internal network;

3. checking web pages for malicious code;

e) defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use and reporting;
f) preparing plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements;

g) implementing procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code;

h) implementing procedures to verify information relating to malicious code, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, are used to differentiate between hoaxes and real malicious code; all users must be made aware of the problem of hoaxes and what to do on receipt of them.

**9.4.2 Controls against mobile code**

Control: Where the use of mobile code is authorised, the configuration must ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code must be prevented from executing.

The following should be implemented to protect against mobile code performing unauthorised actions:

a) executing mobile code in a logically isolated environment;

b) blocking any use of mobile code;

c) blocking receipt of mobile code;

d) activating technical measures as available on a specific system to ensure mobile code is managed;

e) control the resources available to mobile code access;

f) cryptographic controls to uniquely authenticate mobile code.

---

10 Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction (e.g. ActiveX, Java applets, JavaScript). Mobile code is associated with a number of middleware services.
9.5 Back-up

**Objective**: To maintain the integrity and availability of information and information processing facilities.

Routine procedures must be established to implement the agreed back-up policy and strategy for taking back-up copies of data and rehearsing their timely restoration.

9.5.1 Information backup

**Control**: Backup copies of information and software must be taken and tested regularly in accordance with the agreed backup policy.

Adequate backup facilities must be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information backup must be implemented:

a) the necessary level of backup information must be defined in a backup policy;

b) accurate and complete records of the back-up copies and documented restoration procedures must be produced;

c) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements, the security requirements of the information involved, and the criticality of the information to the continued operation of the service;

d) the backups must be stored in a remote location with a different risk profile to escape any damage from a disaster at the main site;

e) backup information must be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the backup site;

f) backup media must be tested to ensure that they can be relied upon for emergency use when necessary;

g) restoration procedures must be regularly checked and tested (*Restoration Check Interval*) to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;

h) in situations where confidentiality is of importance, backups should be protected by means of encryption;

i) the retention period for essential business information, and also any requirement for archive copies to be permanently retained must be determined.
9.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

The secure management of networks, which may span the boundaries of the service providing organisation, requires careful consideration to dataflow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

9.6.1 Network controls

Control: Networks must be adequately managed and controlled in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Network managers must implement controls to ensure the security of information in networks, and the protection of connected services from unauthorised access. The following items must be implemented:

a) operational responsibility for networks should be separated from computer operations where appropriate;

b) responsibilities and procedures for the management of remote equipment, including equipment in user areas, must be established;

c) logging and monitoring should be applied to enable recording of security relevant actions;

d) management activities should be closely co-ordinated both to optimise the service and to ensure that controls are consistently applied across the information processing infrastructure.
9.6.2 Security of network services

Control: Security features, service levels, and management requirements of all network services\textsuperscript{11} must be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

The ability of the network service provider to manage agreed services in a secure way must be determined and monitored, and the right to audit must be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, must be identified and included in the contract.

9.7 Media handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

Media must be controlled and physically protected.

Operating procedures must be established to protect documents, computer media (e.g. tapes, disks, memory sticks, CDs, DVDs), input/output data and system documentation from unauthorised disclosure, modification, removal, and destruction.

9.7.1 Management of removable media

Control: There must be procedures in place for the management of removable media\textsuperscript{12}.

The following measures for the management of removable media must be implemented:

a) if no longer required, the contents of any re-usable media that are to be removed from the hosting premises must be made unrecoverable;

b) where necessary and practical, authorisation should be required for media removed from the hosting premises and a record of such removals must be kept in order to maintain an audit trail;

c) all media must be stored in a safe, secure environment, in accordance with manufacturers’ specifications;

\textsuperscript{11} Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems. Network services are for example SWIFT, Internet access, mail service provider, etc.

\textsuperscript{12} Removable media include e.g. tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.
d) information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers’ specifications) must be also stored elsewhere to avoid information loss due to media degradation;

e) registration of removable media must be implemented to limit the opportunity for data loss.

f) all procedures and authorisation levels must be clearly documented.

9.7.2 Disposal of media

Control: Media must be disposed of securely and safely when no longer required, using formal procedures.

Formal procedures for the secure disposal of media should minimise the risk of sensitive information leakage to unauthorised persons. The procedures for secure disposal of media containing sensitive information must be commensurate with the sensitivity of that information. The following items must be implemented:

a) media containing sensitive information must be stored and disposed of securely and safely, e.g. by incineration or shredding, or erased of data for use by another application;

b) procedures must be in place to identify the items that might require secure disposal;

c) care must be taken in selecting a contractor that provide disposal services for papers, equipment and media;

d) disposal of sensitive items must be logged in order to maintain an audit trail.

9.7.3 Information handling procedures

Control: Procedures for the handling and storage of information must be established to protect this information from unauthorised disclosure or misuse.

Procedures must be drawn up for handling, processing, storing, and communicating information consistent with its classification. The following items must be implemented:

a) handling and labelling of all media to its indicated classification level;

b) access restrictions to prevent access from unauthorised personnel;

c) maintenance of a formal record of the authorised recipients of data;

These procedures apply to information in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of facsimile machines.
d) protection of spooled data awaiting output to a level consistent with its sensitivity;

e) storage of media in accordance with manufacturers’ specifications;

f) keeping the distribution of data to a minimum (need-to-know principle);

g) clear marking of all copies of media for the attention of the authorised recipient;

h) review of distribution lists and lists of authorised recipients at planned intervals

(Distribution List Review Interval).

9.7.4 Security of system documentation

Control: System documentation must be protected against unauthorised access.

To secure system documentation, the following items must be implemented:

a) system documentation must be stored securely;

b) access to system documentation must be limited to authorised persons;

c) system documentation held on a public network, or supplied via a public network, must

be protected.

9.8 Exchange of information and software

Objective: To maintain the security of information and software exchanged within the service

providing organisation and with any external entity.

Exchange of information and software between the service providing organisation and an

external entity must be based on a formal exchange policy, carried out in line with exchange

agreements, and must be compliant with any relevant legislation.

Procedures must be established to protect information and physical media containing information

in transit.

9.8.1 Information exchange policies and procedures

Control: Formal exchange policies, procedures, and controls must be in place to protect the

exchange of information through the use of all types of communication facilities.

14 System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, authorisation processes.
The procedures and controls to be followed when using electronic communication facilities for information exchange should consider the following items:

a) procedures designed to protect exchanged information from interception, copying, modification, mis-routing, and destruction;

b) procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications;

c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

d) policy or guidelines outlining acceptable use of electronic communication facilities;

e) procedures for the use of wireless communications, taking into account the particular risks involved;

f) employee, contractor and any other user’s responsibilities not to compromise the service providing organisation, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorised purchasing, etc.;

g) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information;

h) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

i) not leaving sensitive or critical information on printing facilities, e.g. copiers, printers, and facsimile machines, as these may be accessed by unauthorised personnel;

j) controls and restrictions associated with the forwarding of communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

k) reminding personnel that they should take precautions, e.g. not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by:

1. people in their immediate vicinity particularly when using mobile phones;

2. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers;

3. people at the recipient’s end;

l) not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorised persons, stored on communal systems or stored incorrectly as a result of misdialling;
reminding personnel about the problems of using facsimile machines, namely:

1. unauthorised access to built-in message stores to retrieve messages;
2. deliberate or accidental programming of machines to send messages to specific numbers;
3. sending documents and messages to the wrong number either by misdialling or using the wrong stored number;

reminding personnel not to register demographic data, such as the e-mail address or other personal information, in any software to avoid collection for unauthorised use;

reminding personnel that modern facsimile machines and photocopiers have page caches and store pages in case of a paper or transmission fault, which will be printed once the fault is cleared.

In addition, personnel should be reminded that they should not have confidential conversations in public places or open offices and meeting places with non-sound proofed-walls.

Information exchange facilities must comply with any relevant legal requirements.

9.8.2 Exchange agreements

Control: Agreements must be established for the exchange of information and software between the service providing organisation and external parties (see also control 5.2.1).

Exchange agreements should, if applicable, consider the following security conditions:

a) management responsibilities for controlling and notifying transmission, dispatch, and receipt;

b) procedures for notifying sender of transmission, dispatch, and receipt;

c) procedures to ensure traceability and non-repudiation;

d) minimum technical standards for packaging and transmission;

e) escrow agreements\(^{15}\);

f) courier identification standards;

\(^{15}\) A legal provision whereby, in the event of a developer/supplier failing or otherwise ceasing to trade, the source code for their packaged software is made available to licensed / registered users, thereby enabling its ongoing maintenance.
g) responsibilities and liabilities in the event of information security incidents, such as loss of data;

h) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is protected;

i) ownership and responsibilities for data protection, copyright, software license compliance and similar considerations;

j) technical standards for recording and reading information and software;

k) any special controls that may be required to protect sensitive items, such as cryptographic keys.

9.8.3 Physical media in transit

Control: Media containing information must be protected against unauthorised access, misuse or corruption during transportation outside the hosting premises.

The following measures must be implemented to protect information media being transported between sites:

a) reliable transport or couriers must be used;

b) a list of authorised couriers must be established;

c) procedures to check the identification of couriers must be developed;

d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers’ specifications, for example protecting software against any environmental factors that may reduce the media’s restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;

e) controls should be adopted, where necessary, to protect sensitive information from unauthorised disclosure or modification; examples include:

1. use of locked containers;

2. delivery by hand;

3. tamper-evident packaging (which reveals any attempt to gain access);

4. in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.
9.8.4 Electronic messaging

Control: Information involved in electronic messaging must be protected.

Security considerations for electronic messaging must include the following:

a) protecting messages from unauthorised access, modification or denial of service;

b) ensuring correct addressing and transportation of the message;

c) general reliability and availability of the service;

d) legal considerations, for example requirements for electronic signatures;

e) obtaining approval prior to using external public services such as instant messaging or file sharing;

f) stronger levels of authentication controlling access from publicly accessible networks.

9.8.5 Business Information Systems

Control: Policies and procedures must be developed and implemented to protect the service’s information associated with the interconnection of business/office information systems.

Office information systems are opportunities for faster dissemination and sharing of service related information using a combination of: documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and facsimile machines. Consideration given to the security and business implications of interconnecting such facilities must include:

a) vulnerabilities in systems where information extracted from the service (e.g. statistical data) is shared between different parts of the service providing organization;

b) vulnerabilities of information in business communication systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail;

c) policy and appropriate controls to manage information sharing within the service providing organisation;

d) restricting access to diary information relating to selected individuals, e.g. personnel working on sensitive projects;

e) restricting selected facilities (e.g. functional mail boxes, document management systems) to specific categories of user;
f) identifying the status of office information system users, e.g. employees of the organization or contractors in directories for the benefit of other users;

9.9 Electronic commerce services

Objective: To ensure that the integrity and availability of information electronically published through publicly available systems is considered.

9.9.1 Publicly available information

Control: The integrity of information being made available on a publicly available system must be protected to prevent unauthorised modification.

Software, data, and other information requiring a high level of integrity, being made available on a publicly available system (e.g. information on a Web server accessible via the Internet), must be protected by appropriate mechanisms, e.g. digital signatures. The publicly accessible system must be tested against weaknesses and failures prior to information being made available.

There must be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system must be verified and approved.

Electronic publishing systems, especially those that permit feedback and direct entering of information, must be carefully controlled so that:

- information is obtained in compliance with any data protection legislation;
- information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;
- sensitive information will be protected during collection, processing, and storage;
- access to the publishing system does not allow unintended access to networks to which the system is connected.

9.10 Monitoring

Objective: To detect unauthorised information processing activities.

Systems must be monitored and information security events must be recorded. Operator logs and fault logging must be used to ensure information system problems are identified.

The service providing organisation must comply with all relevant legal requirements applicable to its monitoring and logging activities.
9.10.1 Audit logging

Control: Audit logs recording user activities, exceptions, and information security events must be produced and kept for an agreed period (Audit Logging Period) to assist in future investigations and access control monitoring.

Audit logs must include:

a) user IDs;
b) dates, times, and details of key events, e.g. log-on, failed log-on attempts and log-off;
c) terminal identity or location if possible;
d) records of rejected data and other resource access attempts;
e) changes to system configuration;
f) use of privileges;
g) use of system utilities and applications (if such features are provided);
h) files accessed and the kind of access according to the classification;
i) network addresses and protocols according to the classification;
j) alarms raised by the access control system;
k) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

9.10.2 Monitoring system use

Control: Procedures for monitoring use of information processing facilities must be established by senior management and the results of the monitoring activities reviewed regularly.

The level of monitoring required and the intervals for individual facilities must be determined by a risk assessment. The service providing organisation must comply with all relevant legal requirements applicable to its monitoring activities. Events that must be monitored are:

a) authorised access to critical data such as:
   1) the user ID;
   2) the date and time of key events;
   3) the types of events;
   4) the files accessed;
5) the program/utilities used;

b) all privileged operations such as:

1) use of privileged accounts, e.g. supervisor, root, administrator;

2) system start-up and stop;

3) I/O device attachment/detachment;

c) unauthorised access attempts such as:

1) failed or rejected user actions;

2) failed or rejected actions involving data and other resources;

3) access policy violations and notifications for network gateways and firewalls;

4) alerts from proprietary intrusion detection systems;

d) system alerts or failures such as:

1) console alerts or messages;

2) system log exceptions;

3) network management alarms;

4) alarms raised by the access control system;

e) changes to, or attempts to change, system security settings and controls.

The above events must be reviewed at planned intervals (Privileged Activities Review Interval).

9.10.3 Protection of log information

Control: Logging facilities and log information must be protected against tampering and unauthorised access.

Controls should aim to protect against unauthorised changes and operational problems with the logging facility including:

a) alterations to the message types that are recorded;

b) log files being edited or deleted;

c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence.
9.10.4 Administrator and operator logs

Control: System administrator and system operator activities must be logged.

Logs should include:

a) the time at which an event (success or failure) occurred;
b) information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);
c) which account and which administrator or operator was involved;
d) which processes were involved.

System administrator and operator logs must be reviewed at planned intervals (Administrator Log Review Interval).

9.10.5 Fault logging

Control: Faults must be logged, analysed, and appropriate action taken.

Faults reported by users or by system programs related to problems with information processing or communications systems must be logged. There must be clear rules for handling reported faults including:

a) review of fault logs to ensure that faults have been satisfactorily resolved;
b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorised.

It must be ensured that error logging is enabled, if this system function is available.

The level of logging required for individual systems must be determined by a risk assessment, taking performance degradation into account.

9.10.6 Clock synchronisation

Control: The clocks of all information processing systems (belonging to the service) must be synchronised with an agreed accurate time source.

For computers or communication devices which have the capability to operate a real-time clock, this clock must be set to an agreed standard, e.g. Coordinated Universal Time (UTC) or local standard time. As some clocks are known to drift with time, there must be a procedure that checks for and corrects any significant variation.
10 Access control

10.1 Business requirement for access control

Objective: To control access to information.

Access to information, information processing facilities, and business processes must be controlled on the basis of business and security requirements. Access control rules must take account of policies for information dissemination and authorisation.

10.1.1 Access control policy

Control: An access control policy must be established, documented, and reviewed based on business and security requirements for access.

Access control rules and rights for each user or group of users must be clearly stated in an access control policy. Access controls are both logical and physical and these should be implemented together since they complement each other. Users and service providers must be given a clear statement of the business requirements to be met by access controls.

The policy must take account of the following:

- security requirements of individual business applications;
- identification of all information related to the business applications and the risks the information is facing;
- policies for information dissemination and authorisation, e.g. the need to know principle and security levels and classification of information;
- consistency between the access control and information classification policies of different systems and networks;
- relevant legislation and any contractual obligations regarding protection of access to data or services;
- standard user access profiles for common job roles;
- management of access rights in a distributed and networked environment which recognises all types of connections available;
- segregation of access control roles, e.g. access request, access authorisation, access administration;
- requirements for formal authorisation of access requests;
j) requirements for periodic review of access controls;

k) removal of access rights.

The policy should be reviewed at planned intervals (User Access Control Policy Review Interval).

10.2 User access management

Objective: To ensure authorised user access and prevent unauthorised access to information systems.

Formal procedures must be in place to control the allocation of access rights to information systems and services.

The procedures must cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given to the need to control the allocation of privileged access rights, which allow users to override system controls.

10.2.1 User registration

Control: There must be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems (belonging to the service) and services.

The access control procedure for user registration and de-registration must include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and must be approved and documented;

b) checking that the user has authorisation from relevant management for the use of the information system or service;

c) checking that the level of access granted is appropriate to the business purpose and is consistent with organisational security policy, e.g. it does not compromise segregation of duties;

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorisation procedures have been completed;
g) maintaining a formal record of all persons registered to use the service;

h) immediately removing or blocking access rights of users who have changed roles or jobs or have left;

i) checking for, and removing or blocking, redundant user IDs and accounts;

j) ensuring that redundant user IDs are not issued to other users.

10.2.2 Privilege management

Control: The allocation and use of privileges must be restricted and controlled.

The allocation of privileges must be controlled through a formal authorisation process. The following steps must be implemented:

a) the access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated must be identified and documented;

b) Privileges must be allocated to individuals on a need-to-use basis for the normal operating and on an event-by-event basis for exceptional situations;

c) an authorisation process and a record of all privileges allocated must be maintained. Privileges must not be granted until the authorisation process is complete;

d) privileges should be assigned to a different user ID from those used for normal business use.

10.2.3 User password management

Control: The allocation of passwords must be controlled through a formal management process.

The process must include the following requirements:

a) users must be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group;

b) when users are required to maintain their own passwords they must be provided initially with a secure temporary password, which they are forced to change immediately;

c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;

d) temporary passwords must be given to users in a secure manner;

e) temporary passwords must be unique to an individual and should not be guessable;
f) users must acknowledge receipt of passwords;

g) passwords must never be stored on computer systems in an unprotected form;

h) default vendor passwords must be altered following installation of systems or software.

10.2.4 Review of user access rights

Control: Management must review users’ access rights at regular intervals using a formal process.

The review of access rights according to the following points must be in place:

a) users’ access rights must be periodically reviewed (User Access Rights Review Interval);

b) user access rights must be reviewed and re-allocated when moving from one employment to another within the same central bank;

c) authorisations for special privileged access rights must be periodically reviewed (Privileged User Access Rights Review Interval);

d) changes to privileged accounts must be logged for periodic review (Privileged Account Changes Logging Period).

10.3 User responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

As the co-operation of authorised users is essential for effective security they must be made aware of their responsibilities for maintaining effective access controls.

A clear desk and clear screen policy must be implemented to reduce the risk of unauthorised access or damage to papers, media, and information processing facilities.
10.3.1 Password use

Control: Users must be required to follow the password policy and good security practices in the selection and use of passwords. The software providing the authentication facilities should support parameters\(^\text{16}\) to ensure strong passwords.

All users must at least:

- a) keep passwords confidential;
- b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;
- c) change passwords whenever there is any indication of possible system or password compromise;
- d) not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- e) not share individual user passwords.

In accordance with the password policy the service must ensure that:

- a) user account names have at least the minimum length;
- b) quality passwords with sufficient complexity and minimum length (Minimum Password Length) are selected;
- c) password change is enforced after expiry (Password Expiry Period) and at the first log-on for temporary passwords;
- d) reuse or recycle a certain number of old passwords is prevented;
- e) user accounts are locked after a certain number of failed login attempts (Maximum Logon Attempts).

10.3.2 Unattended user equipment

Control: Users must ensure that unattended equipment has appropriate protection.

\(^\text{16}\) Authentication parameters define settings required for login security. Examples are: Password Expiry (defining the maximum number of calendar days a password is valid), Minimum Account Name / Password Length (minimum number of characters allowed for a account name/password), Password Complexity (defining the minimum complexity of the password – e.g. at least one uppercase character, one symbol and one number), Password Reuse (defines the number of password changes before an old password can be reused), Maximum Login Attempts (maximum number of failed login attempts before a user account is locked by the system)
All users must be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users must be advised to:

a) terminate active sessions when finished, unless they can be secured by a locking mechanism, e.g. a password protected screen saver;

b) log-off from mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);

c) secure PCs or terminals from unauthorised use by a key lock or an equivalent control, e.g. password access, when not in use.

10.3.3 Clear desk and clear screen policy

Control: A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities must be adopted.

The clear desk and clear screen policy must take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects. The following measures must be implemented:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, must be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;

b) computers and terminals must be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and must be protected by key locks, passwords or other controls when not in use;

c) incoming and outgoing mail points and unattended facsimile machines must be protected;

d) unauthorised use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) should be prevented;

e) documents containing sensitive or classified information must be removed from printers immediately.

10.4 Network access control

Objective: To prevent unauthorised access to networked services.
1546 Access to both internal and external networked services must be controlled.
1547 User access to networks and network services must not compromise the security of the network services by ensuring:
1548 a) appropriate interfaces are in place between the network supporting the service and networks operated by other organisations, and public networks;
1550 b) appropriate authentication mechanisms are applied for users and equipment;
1552 c) control of user access to information services is enforced.
1553
1554 **10.4.1 Policy on use of network services**
1555 Control: Users must only be provided with access to those services that they have been specifically authorised to use.
1556 A policy must be formulated concerning the use of networks and network services. This policy must cover:
1558 a) the networks and network services which are allowed to be accessed;
1559 b) authorisation procedures for determining who is allowed to access which networks and network services;
1561 c) management controls and procedures to protect access to network connections and network services;
1563 d) the means used to access networks and network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).
1565 The policy on the use of network services must be consistent with the business access control policy.
1567 **10.4.2 User authentication for external connections**
1568 Control: Strong authentication methods (e.g. hardware token, certificates) must be used to control access by remote users.\(^{17}\)
1570 A formal procedure for managing and controlling remote connections must be established.
1571 Following controls must be in place:

\(^{17}\) a user trying to establish a connection from a location outside of the information processing facilities
a) Remote connections must only be activated when absolutely necessary and ask for re-authentication after a defined period of inactivity (Remote Connections Idle Interval);  
b) authentication by the use of cryptographic techniques and two-factor authentication;  
c) If used, call-back facilities, must follow strict controls and procedures; call forwarding processes should only be used if absolutely necessary;  
d) A logging of all remote connections must be in place.

If remote connections are used for Third Party/vendor support  
a) the decision to allow remote access by TP/vendors is made case by case by the senior management and substantiated by a risk analysis;  
b) remote access must be allowed only for a limited period of time and only in case support can not be provided on site in time;  
c) contractual provisions for remote access must exist and must also be laid down as regards the commitment of vendors’ personnel to the secrecy of data;  
d) access should be limited to read-only for diagnostic purposes. However, if more privileged access is required (e.g. in emergency cases) then the remote connection activity related to critical functions must be monitored;  
e) if used, call-back facilities, must follow strict controls and procedures; call forwarding processes should only be used if absolutely necessary;  
f) a logging of all remote connections must be in place.

10.4.3 Equipment identification in networks  
Control: Automatic equipment identification must be implemented as a means to authenticate connections from specific locations and equipment.

10.4.4 Remote diagnostic and configuration port protection  
Control: Physical and logical access to diagnostic and configuration ports must be controlled.

Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port.

Ports, services, and similar facilities installed on a computer or network facility, which is not specifically required for business functionality, must be disabled or removed.
10.4.5  Segregation in networks

Control: Groups of information services, users, and information systems must be segregated from a logical point of view.

The security of the network must be controlled by dividing it into separate (physical or logical) network domains. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

The criteria for segregation of networks into domains must be based on the access control policy and access requirements, and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

In addition, segregation of networks must be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

10.4.6  Network connection control

Control: The capability of users to connect to the network must be restricted, in line with the access control policy and requirements of the business applications.

The network access rights of users must be maintained and updated as required by the access control policy.

Linking network access rights to certain times of day or dates should be implemented.

10.4.7  Network routing control

Control: Routing controls must be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Routing controls must be based on positive checks of source and destination address.

10.5  Operating system access control

Objective: To prevent unauthorised access to operating systems.

Security facilities must be used to restrict access to operating systems to authorised users. Access must be granted based on the “need-to-have” principle.

10.5.1  Secure log-on procedures

Control: Access to operating systems must be controlled by a secure log-on procedure.
The procedure for logging into an operating system must be designed to minimise the opportunity
for unauthorised access. The log-on procedure must therefore disclose the minimum of
information about the system, in order to avoid providing an unauthorised user with any
unnecessary assistance. A good log-on procedure must:

a) not display system or application identifiers until the log-on process has been
   successfully completed;

b) display a general notice warning that the computer should only be accessed by authorised
   users;

c) not provide help messages during the log-on procedure that would aid an unauthorised
   user;

d) validate the log-on information only on completion of all input data. If an error condition
   arises, the system should not indicate which part of the data is correct or incorrect;

e) limit the number of unsuccessful log-on attempts allowed, to four bad log-on attempts,
   and consider:
   1. recording unsuccessful and successful attempts;
   2. disconnecting connections;
   3. sending an alarm message to the system console if the maximum number of log-on
      attempts is reached.

f) limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the
   system should terminate the log-on;

g) display the following information on completion of a successful log-on:
   1. date and time of the previous successful log-on;
   2. details of any unsuccessful log-on attempts since the last successful log-on;

h) not display the password being entered or consider hiding the password characters by
   symbols;

i) not transmit passwords in clear text over a network.

j) forcing a time delay before further log-on attempts are allowed or rejecting any further
   attempts without specific authorisation.
10.5.2 User identification and authentication

Control: All users must have a unique identifier (user ID) for their personal use only, and a suitable authentication technique must be chosen to substantiate the claimed identity of a user.

This control must be applied for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators).

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management must be documented for such cases. Additional controls are required to maintain accountability.

Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g. read only access), or where there are other controls in place (e.g. password for a generic ID only issued to one staff at a time and logging such instance).

Strong authentication and identity verification is required for staff having access to processing facilities via a remote connection (i.e. via unsecured networks), authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, must be used.

10.5.3 Password management system

Control: Systems for managing passwords must be interactive and must ensure quality passwords in line with the security control 10.3.1.

A password management system must:

a) enforce the use of individual user IDs to maintain accountability;

b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

c) enforce a choice of quality passwords;

d) enforce password changes;

e) force users to change temporary passwords at the first log-on;

f) maintain a record of previous user passwords for a defined minimum period of time and prevent re-use (Period for Keeping Previous Passwords);

g) not display passwords on the screen when being entered;

h) store password files separately from application system data;
i) store and transmit passwords in protected (e.g. encrypted or hashed) form.

10.5.4 Use of system utilities

Control: The use of utility programs (e.g. security tools, SQL, QMF, APF) that might be capable of overriding system and application controls must be restricted and tightly controlled.

The following measures for the use of system utilities must be implemented:

a) use of identification, authentication, and authorisation procedures for system utilities;

b) segregation of system utilities from applications software;

c) limitation of the use of system utilities to the minimum practical number of trusted, authorised users;

d) authorisation for ad hoc use of systems utilities;

e) logging of all use of system utilities;

f) defining and documenting of authorisation levels for system utilities;

g) removal or disabling of all unnecessary software based utilities and system software;

h) not making system utilities available to users who have access to applications on systems where segregation of duties is required.

10.5.5 Session time-out

Control: Inactive sessions must shut down after a defined period of inactivity to prevent unauthorised access.

A time-out facility must clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity (Session Time-out).

10.5.6 Limitation of connection time

Control: Restrictions on connection times must be considered to provide additional security for high-risk applications.

Connection time controls should be considered, especially from high risk locations, e.g. external areas that are outside the organization’s security management. Examples of such restrictions include:

a) using predetermined time slots;

b) restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation;
c) considering re-authentication at timed intervals.

10.6 Application and information access control

Objective: To prevent unauthorised access to information held in application systems.

Security facilities must be used to restrict access to and within application systems.

Logical access to application software and information must be restricted to authorised users.

10.6.1 Information access restriction

Control: Access to information and application system functions must be restricted in accordance with the defined access control policy.

Restrictions to access must be based on individual business application requirements. The access control policy must also be consistent with the organisational access policy.

The following measures must be implemented in order to support access restriction requirements:

a) providing menus to control access to application system functions;

b) controlling the access rights of users, e.g. read, write, delete, and execute;

c) controlling access rights of other applications;

d) ensuring that outputs from application systems handling sensitive information contain only the information relevant to the use of the output and are sent only to authorised terminals and locations; this must include periodic reviews of such outputs to ensure that redundant information is removed (Information Access Restriction Review Interval).

10.6.2 Sensitive system isolation

Control: The service must be operated in a dedicated (isolated) computing environment.

A dedicated environment could be achieved using physical or logical methods.

10.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

The protection required must be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should
be considered and appropriate protection applied. In the case of teleworking the respective site
must be appropriately protected and it must be ensured that suitable arrangements are in place for
this way of working.

10.7.1 Mobile computing and communications

Control: A formal policy must be in place, and security measures must be adopted to protect
against the risks of using mobile computing and communication facilities.

The mobile computing policy must include the requirements for physical protection, access
controls, cryptographic techniques, backups, and virus protection. This policy must also include
rules and advice on connecting mobile facilities to networks and guidance on the use of these
facilities in public places.

Procedures against malicious software must be in place and be kept up to date.

Backups of critical business information must be taken regularly. Equipment must be available to
enable the quick and easy backup of information. These backups must be given adequate
protection against, e.g., theft or loss of information.

Suitable protection must be given to the use of mobile facilities connected to networks. Remote
access to business information across public network using mobile computing facilities must only
take place after successful identification and two-factor authentication.

Mobile computing facilities must also be physically protected against theft especially when left
outside the hosting premises, for example, in cars and other forms of transport, hotel rooms,
conference centres, and meeting places. A specific procedure taking into account legal, insurance
and other security requirements of the service providing organisation must be established for
cases of theft or loss of the mobile computing facilities. Equipment carrying important, sensitive,
and/or critical business information must not be left unattended and, where possible, should be
physically locked away, or have special locks (e.g. putting it in a safe) that secure the equipment.

Training must be arranged for personnel using mobile computing to raise their awareness on the
additional risks resulting from this way of working and the controls that should be implemented.

10.7.2 Teleworking

Control: A policy, operational plans and procedures must be developed and implemented for
teleworking activities.

Teleworking activities must both be authorised and controlled by management, and it must be
ensured that suitable arrangements are in place for this way of working.
The following matters should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system;

d) the threat of unauthorised access to information or resources from other persons using the accommodation, e.g. family and friends;

e) the use of home networks and requirements or restrictions on the configuration of wireless network services;

f) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

g) access to privately owned equipment (to check the security of the machine or during an investigation), which may be prevented by legislation;

h) software licensing agreements that are such that the service providing organisation may become liable for licensing for client software on workstations owned privately by employees, contractors or third party users;

i) anti-virus protection and firewall requirements.

The guidelines and arrangements to be implemented should include:

a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the service providing organisation is not allowed;

b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorised to access;

c) the provision of suitable communication equipment, including methods for securing remote access;

d) physical security;

e) rules and guidance on family and visitor access to equipment and information;

f) the provision of hardware and software support and maintenance;
g) the provision of insurance;

h) the procedures for backup and business continuity;

i) audit and security monitoring;

j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

11 Information systems acquisition, development and maintenance

11.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements must be identified, agreed prior to the development and/or implementation of information systems and documented as part of the overall business case for an information system.

11.1.1 Security requirements analysis and specification

Control: Statements of business requirements for new information systems, or enhancements to existing information systems must specify the requirements for security controls. Security requirements and controls must reflect the business value of the information assets involved, and the potential business damage, which might result from a failure or absence of security.

System requirements for information security and processes for implementing security must be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

If products are purchased, a formal testing and acquisition process must be followed. Contracts with the supplier must address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement then the risk introduced and associated controls must be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this must be disabled or the
proposed control structure must be reviewed to determine if advantage can be taken of the enhanced functionality available.

11.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

Controls must be designed into applications, including user developed applications to ensure correct processing. These controls must include the validation of input data, internal processing and output data.

Additional controls may be required for components of the service that process, or have an impact on, sensitive, valuable or critical information. Such controls must be determined on the basis of a risk assessment.

11.2.1 Input data validation

Control: Data input to applications must be validated to ensure that this data is correct and appropriate.

Checks must be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. opening hours). The following checks should be implemented:

a) dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
   1. out-of-range values;
   2. invalid characters in data fields;
   3. missing or incomplete data;
   4. exceeding upper and lower data volume limits;
   5. unauthorised or inconsistent control data;

b) periodic review of the content of key fields or data files to confirm their validity and integrity;

c) procedures for responding to validation errors;

d) procedures for testing the plausibility of the input data;

e) creating a log of the activities involved in the data input process.
11.2.2 Control of internal processing

Control: Validation checks must be incorporated into applications to detect any corruption of information through processing errors or deliberate acts. The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimised. Specific areas to consider include:

a) the use of add, modify, and delete functions to implement changes to data;
b) the procedures to prevent programs running in the wrong order or running after failure of prior processing;
c) the use of appropriate programs to recover from failures to ensure the correct processing of data;
d) protection against attacks using buffer overruns/overflows.

A checklist must be prepared, activities documented, and the results must be kept secure. Examples of checks that can be incorporated include the following:

a) session or batch controls, to reconcile data file balances after transaction updates;
b) balancing controls, to check opening balances against previous closing balances, namely:
   1. run-to-run controls;
   2. file update totals;
   3. program-to-program controls;
c) validation of system-generated input data;
d) checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers;
e) hash totals of records and files;
f) checks to ensure that application programs are run at the correct time;
g) checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved;
h) creating a log of the activities involved in the processing.

11.2.3 Message integrity

Control: Requirements for ensuring authenticity and protecting message integrity in applications must be identified, and controls identified and implemented.
An assessment of security risks must be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

11.2.4 Output data validation

Control: Data output from an application must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Output validation may include:

a) plausibility checks to test whether the output data is reasonable;

b) reconciliation control counts to ensure processing of all data;

c) procedures for responding to output validation tests;

d) creating a log of activities in the data output validation process.

11.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

A policy must be developed on the use of cryptographic controls. Key management must be in place to support the use of cryptographic techniques.

11.3.1 Policy on the use of cryptographic controls

Control: A policy on the use of cryptographic controls for protection of information must be developed and implemented.

When developing a cryptographic policy the following measures must be implemented:

a) the management approach towards the use of cryptographic controls across the service, including the general principles under which business information must be protected;

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm required;

---

18 Cryptographic controls can be used to achieve different security objectives, e.g.: a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted; b) integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information; c) non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non occurrence of an event or action.
c) the use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines;

d) the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e) roles and responsibilities, e.g. who is responsible for:

1. the implementation of the policy;

2. the key management, including key generation;

f) the standards to be adopted for the effective implementation throughout the service (which solution is used for which business processes);

g) the impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).

When implementing the cryptographic policy for the service, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of Europe and to the issues of trans-border flow of encrypted information.

11.3.2 Key management

Control: Key management must be in place to support the use of cryptographic techniques.

All cryptographic keys must be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorised disclosure. Equipment used to generate, store and archive keys must be physically protected.

A key management system must be based on an agreed set of standards, procedures, and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) generating and obtaining public key certificates;

c) distributing keys to intended users, including how keys should be activated when received;

d) storing keys, including how authorised users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;
g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves (in which case keys should also be archived);

h) recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;

i) archiving keys, e.g. for information archived or backed up;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys must be defined so that the keys can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

In addition to securely managing secret and private keys, the authenticity of public keys must also be implemented.

11.4 Security of system files

Objective: To ensure the security of system files.

Access to system files and program source code must be controlled. Ensure that IT projects and support activities conducted in a secure manner. Care must be taken to avoid exposure of sensitive data in test environments.

11.4.1 Control of operational software

Control: There must be procedures in place to control the installation of software components on operational systems.

To minimise the risk of corruption to operational systems, the following measures must be implemented to control changes:

a) the updating of the operational software, applications, and program libraries must only be performed by trained administrators upon management authorisation;

b) operational systems should only hold approved executable code, and not development code or compilers;

c) applications and operating system software must only be implemented after extensive and successful testing; the tests must include tests on usability, security, effects on other
systems and user-friendliness, and should be carried out on separate systems; it must be
guaranteed that all corresponding program source libraries have been updated;
d) a configuration control system must be used to keep control of all implemented software
as well as the system documentation;
e) a rollback strategy must be in place before changes are implemented;
f) an audit log must be maintained of all updates to operational program libraries;
g) the previous version of application software must be retained as a contingency measure;
h) old versions of software (including system management software, scripts) must be
archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in
archive.

Vendor supplied software used in operational systems must be maintained at a level supported by
the supplier. Over time, software vendors will cease to support older versions of software. The
senior management must consider the risks of relying on unsupported software.

Any decision to upgrade to a new release must take into account the business requirements for
the change, and the security of the release, i.e. the introduction of new security functionality or
the number and severity of security problems affecting this version. Software patches must be
applied when they can help to remove or reduce security weaknesses.

Physical or logical access must only be given to suppliers for support purposes when necessary,
and with management approval. The supplier’s activities must be monitored.

11.4.2 Protection of system test data

Control: Test data must be selected carefully. If sensitive information is used for testing purposes, it must be protected and controlled.

The use of operational databases containing personal information or any other sensitive information for testing purposes should be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content must be removed or modified beyond
recognition before use. The following guidelines must be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, should also apply to test application systems;
b) there must be separate authorisation each time operational information is copied to a test application system;

c) operational information must be erased from a test application system immediately after the testing is complete;

d) the copying and use of operational information must be logged to provide an audit trail.

11.4.3 Access control to program source code

Control: Access to program source code must be restricted according to the senior management’s decision.

Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) must be strictly controlled, in order to prevent the introduction of unauthorised functionality and to avoid unintentional changes. The following measures must then be implemented to control access to such program source libraries/directories in order to reduce the potential for corruption of computer programs:

a) where possible, program source libraries/directories should not be held in operational systems;

b) the program source code and the program source libraries/directories must be managed according to established procedures;

c) support personnel must not have unrestricted access to program source libraries/directories;

d) the updating of program source libraries/directories and associated items, and the issuing of program sources to programmers must only be performed after authorisation has been received;

e) program listings must be held in a secure environment;

f) an audit log must be maintained of all access to program source libraries/directories;

g) maintenance and copying of program source libraries/directories must be subject to strict change control procedures.

11.5 Security in development and support processes

Objective: To maintain the security of application system software and information. Project and support environments must be strictly controlled.
11.5.1 Change control procedures

Control: The implementation of changes\(^\text{19}\) must be controlled by the use of formal change control procedures. Formal change control procedures must be documented and enforced in order to minimise the corruption of information systems. Introduction of new systems and major changes to existing systems must follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process must include a risk assessment, analysis of the impacts of changes, and specification of security controls needed. This process must also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

The change procedures must include:

a) identification and recording of changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including security impacts, of such changes;

d) maintaining a record of agreed authorisation levels;

e) ensuring change requests are submitted by authorised users;

f) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

g) identifying all software, information, database entities, and hardware that require amendment;

h) obtaining formal approval for detailed proposals before work commences;

i) ensuring authorised users accept changes prior to implementation;

j) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

k) ensuring that operating documentation and user procedures are changed as necessary to remain appropriate;

\(^\text{19}\) These changes include not only software, but hardware and procedures as well.
11.5.2 Technical review of applications after operating system changes

Control: Before operating system software is changed, all business-critical applications must be reviewed and tested to ensure that there is no adverse impact on business operations or security.

This process must cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;

c) ensuring that notification of operating system changes is provided in time to allow tests and reviews to take place before implementation;

d) ensuring that appropriate changes are made to the business continuity plans.

11.5.3 Restrictions on changes to software packages

Control: Modifications to software packages must be discouraged, limited to necessary changes, and all changes must be strictly controlled.

As far as possible, and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points must be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) whether the consent of the vendor should be obtained;
c) the possibility of obtaining the required changes from the vendor as standard program updates;

d) the impact if the service providing organisation becomes responsible for the future maintenance of the software as a result of changes.

If changes are necessary the original software must be retained and the changes applied to a clearly identified copy. A software update management process must be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorised software. All changes must be fully tested and documented, so that they can be reapplied if necessary to future software upgrades.

11.5.4 Outsourced software development

Control: Outsourced software development must be supervised and monitored

Where software development is outsourced, the following points must be considered:

a) licensing arrangements, code ownership, and intellectual property rights;

b) certification of the quality and accuracy of the work carried out;

c) escrow arrangements in the event of failure of the third party;

d) rights of access for audit of the quality and accuracy of work done;

e) If open source software is used the following controls must be applied:

1. downloaded from a trusted source

2. integrity check, e.g. MD5 verification

3. verifying the general licensing arrangements (e.g. GNU license)

f) contractual requirements for quality and security functionality of code;

g) testing before installation to detect malicious and Trojan code.

11.5.5 Information leakage

Control: Opportunities for information leakage must be prevented.

As far as possible, and practicable, is has to be ensured that covert channels\textsuperscript{20} and Trojan codes\textsuperscript{21} are not introduced into a new or upgraded system.

\textsuperscript{20} A covert channel can expose information by some indirect and obscure means.

\textsuperscript{21} Trojan code is designed to affect a system in a way that is not authorised.
This control is redundant with 11.5.1 Change control procedures, 9.4.1 Controls against malicious code and 9.4.2 Controls against mobile code.

11.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

Technical vulnerability management must be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations must include operating systems, and any other applications in use.

11.6.1 Control of technical vulnerabilities

Control: Timely information about technical vulnerabilities of information systems being used must be obtained, the exposure of the service to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the organisation responsible for the software.

Timely action must be taken in response to the identification of potential technical vulnerabilities.

The following measures must be implemented to establish an effective management process for technical vulnerabilities:

a) roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any other coordination activities must be clearly defined and established;

b) information resources that will be used to identify technical vulnerabilities and to maintain awareness about them must be identified for software and other technology (based on the asset inventory list); these information resources must be updated based on changes in the inventory, or when other new or useful resources are found;

c) a timeline must be defined to react to notifications of potential technical vulnerabilities;

d) once a potential technical vulnerability has been identified, the senior management must identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems and/or applying other controls;
e) depending on how urgently a technical vulnerability needs to be addressed, the action taken must be carried out according to the controls related to change management or by following information security incident response procedures;

f) if a patch is available, the risks associated with installing the patch must be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);

g) patches must be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be implemented, such as:

1. turning off services or capabilities related to the vulnerability;
2. adapting or adding access controls, e.g. firewalls, at network borders;
3. increased monitoring to detect or prevent actual attacks;
4. raising awareness of the vulnerability;

h) an audit log must be kept for all procedures undertaken;

i) the technical vulnerability management process must be monitored and evaluated in order to ensure its effectiveness and efficiency;

j) system components at high risk must be addressed first.

12 Information security incident management

12.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures must be in place. All employees, contractors and third party users must be made aware of the procedures for reporting the different types of events and weaknesses that might have an impact on the security of assets. They are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

12.1.1 Reporting information security events

Control: Information security events must be reported through appropriate management channels as quickly as possible.
A formal information security event reporting procedure must be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact must be established for the reporting of information security events. It must be ensured that this point of contact is well known, is always available and is able to provide adequate and timely response.

All employees, contractors and third party users must be made aware of their responsibility to report any information security events as quickly as possible. They must also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures must include:

a) suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;

b) information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;

c) the correct behaviour to be undertaken in case of an information security event, i.e.:  
   1. noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour) immediately;  
   2. not carrying out any own action, but immediately reporting to the point of contact;  

d) reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches.

**12.1.2 Reporting security weaknesses**

Control: All employees, contractors and third party users must be required to note and report any observed or suspected security weaknesses in systems or services.

All employees, contractors and third party users must report these matters either to the appropriate point of contact as quickly as possible in order to prevent information security incidents. The reporting mechanism should be easy, accessible, and available. They must be informed that they should not, in any circumstances, attempt to prove a suspected weakness.

**12.2 Management of information security incidents and improvements**

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.
Responsibilities must be clearly allocated and procedures must be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement must be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, it must be collected to ensure compliance with legal requirements.

12.2.1 Responsibilities and procedures

Control: Management responsibilities and procedures must be established to ensure a quick, effective, and orderly response to information security incidents.

In addition to reporting of information security events and weaknesses, the monitoring of systems, alerts, and vulnerabilities must be used to detect information security incidents. The following measures for information security incident management procedures must be implemented:

a) procedures must be established to handle different types of information security incident, including:

1. information system failures and loss of service;
2. malicious code;
3. denial of service;
4. errors resulting from incomplete or inaccurate business data;
5. breaches of confidentiality and integrity;
6. misuse of information systems.

b) in addition to normal contingency plans, the procedures must also cover:

1. analysis and identification of the cause of the incident;
2. containment;
3. planning and implementation of corrective action to prevent recurrence, if necessary;
4. communication with those affected by or involved with recovery from the incident;
5. reporting the action to the appropriate authority;

c) audit trails and similar evidence must be collected and secured, as appropriate, for:
1. internal problem analysis;
2. use as forensic evidence in relation to a potential breach of contract breach or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
3. negotiating for compensation from software and service suppliers;
d) action to recover from security breaches and correct system failures must be carefully and formally controlled.

12.2.2 Learning from information security incidents

Control: There must be mechanisms in place to enable the types, volumes, and impacts of information security incidents to be quantified and monitored.

The information gained from the evaluation of information security incidents must be used to identify recurring or high impact incidents.

12.2.3 Collection of evidence

Control: Where a follow-up action against a person or organisation after an information security incident could lead to legal action (either civil or criminal), evidence must be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Internal procedures must be developed and followed when collecting and presenting admissible evidence for the purposes of disciplinary action.

Any forensics work must only be performed on copies of the evidential material. The integrity of all evidential material must be protected. Copying of evidential material must be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilised must be logged.

13 Business continuity management

13.1 Information security aspects of business continuity management

Objective: To counteract interruptions to the service and to protect critical business processes from the effects of major failures of information systems or disasters, and to ensure their timely resumption.
A business continuity management process must be implemented to minimise the impact on the service and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process must identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability must be subject to a business impact analysis. Business continuity plans must be developed and implemented to ensure timely resumption of essential operations. Information security must be an integral part of the overall business continuity process, and other management processes of the service providing organisation.

Business continuity management must include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

### 13.1.1 Including information security in the business continuity management process

**Control:** A managed process must be developed and maintained for business continuity that addresses the information security requirements needed to ensure business continuity of the service.

The process must bring together the following key elements of business continuity management:

- a) understanding the risks the service is facing in terms of likelihood and impact in time, including an identification and prioritisation of critical business processes;
- b) identifying all the assets involved in critical business processes;
- c) understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the service), and establishing the business objectives of information processing facilities;
- d) identifying sufficient financial, organisational, technical, environmental and human resources to address the identified information security requirements;
e) ensuring the safety of personnel and the protection of information processing facilities and property;

f) formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy;

g) regular testing and updating of the plans and processes put in place;

h) ensuring that the management of business continuity is incorporated in the overall processes and structure of the respective central bank; responsibility for the business continuity management process must be assigned at an appropriate level;

i) ensuring that business continuity arrangements are able to cope with a major loss or inaccessibility of critical staff.

13.1.2 Business continuity and risk assessment

Control: Events that can cause interruptions to business processes must be identified, along with the probability and impact of such interruptions and their consequences for information security.

Information security aspects of business continuity must be based on identifying events (or sequence of events) that can cause interruptions to the service, e.g. equipment failure, human errors, theft, fire, natural disasters and acts of terrorism. This must be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period.

Business continuity risk assessments must be carried out with full involvement from owners of business resources and processes. This assessment must consider all business processes and must not be limited to the information processing facilities, but must include the results specific to information security. It is important to link the different risk aspects together, to obtain a complete picture of the business continuity requirements of the service providing organisation.

The assessment must identify, quantify, and prioritise risks against criteria and objectives relevant to the service providing organisation, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

Depending on the results of the risk assessment, a business continuity strategy must be developed to determine the overall approach to business continuity. Once this strategy has been created, endorsement must be provided by senior management, and a plan created and endorsed to implement this strategy.
13.1.3 Developing and implementing continuity plans including information security

Control: Plans must be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time-scales following interruption to, or failure of, critical business processes.

The business continuity planning process must consider the following:

a) identification and agreement of all responsibilities and business continuity procedures;

b) identification of the acceptable loss of information and services;

c) implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place;

d) definition of procedures for both internal and external communication described in a crisis communication plan;

e) operational procedures to follow pending completion of recovery and restoration;

f) documentation of agreed procedures and processes;

g) education of staff in the agreed procedures and processes, including crisis management;

h) testing and updating of the plans.

The planning process must focus on the following business objectives:

a) Business continuity measures must ensure that all business transactions can be processed with the ‘same day value’ and the business day can be finalised with a defined maximum delay;

b) In a ‘disaster situation’\(^\text{22}\) it must be possible to recover operations from a remote secondary site in line with the recovery times stated in the Service Level Agreement.

The services and resources facilitating this must be identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such

\(^{22}\) Major failure or disaster is understood to mean a serious service interruption which is solved by relocation of the service operations to a second site, physically separate from the primary site. Causes for a major failure can be technical faults, such as lengthy hardware, software or communication failures. Disaster events are fire, flood, explosions, sabotage, evacuation, blockade, terrorist attacks etc.
fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services.

Business continuity plans must address vulnerabilities and therefore may contain sensitive information that needs to be protected. Copies of business continuity plans must be stored in a remote location with a different risk profile to escape any damage from a disaster at the main site. Management must ensure copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site. Other material necessary to execute the business continuity plans must also be stored at the remote location.

If alternative temporary locations are used, the level of implemented security controls at these locations must be equivalent to the main site.

13.1.4 Business continuity planning framework

Control: A single framework of business continuity plans must be maintained to ensure that all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

The business continuity plan must describe the approach for continuity, for example the approach to ensure information or information system availability and security. The plan must also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures, e.g. evacuation plans or fallback arrangements, must be amended as appropriate. Procedures must be included within the change management programme to ensure that business continuity matters are always addressed appropriately.

The business continuity plan must have a specific owner. Emergency procedures, manual fallback plans, and recovery plans must be within the responsibility of the owners of the appropriate business resources or processes involved.

A business continuity planning framework must address the identified information security requirements and consider the following:

a) the conditions for activating the plans which describe the process to be followed (e.g. how to assess the situation, who is to be involved) before each plan is activated;

b) emergency procedures, which describe the actions to be taken following an incident, which jeopardises business operations;
c) fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales;

d) temporary operational procedures to follow pending completion of recovery and restoration;

e) recovery procedures which describe the actions to be taken to return to normal business operations;

f) a maintenance schedule which specifies how and when the plan will be tested;

g) a process for maintaining the plan;

h) awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective;

i) the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives must be nominated as required;

j) the critical assets and resources needed to be able to perform the emergency, fallback and recovery procedures.

13.1.5 Testing, maintaining and re-assessing business continuity plans

Control: The business continuity plans must be tested and updated regularly to ensure that they are up to date and effective.

Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The test schedule for business continuity plan(s) must indicate how and when each element of the plan should be tested. Each element of the plan(s) should be tested at planned intervals (Business Continuity Test Interval).

A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include:

a) table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions);

b) simulations (particularly for training people in their post-incident/crisis management roles);
c) technical recovery testing (ensuring information systems can be restored effectively);
d) testing recovery at an alternate site (running business processes in parallel with recovery
operations away from the main site);
e) tests of supplier facilities and services (ensuring externally provided services and
products will meet the contracted commitment);
f) complete rehearsals (testing that personnel, equipment, facilities, and processes can cope
with interruptions).

The results of tests must be recorded and actions taken to improve the plans, where necessary.

Responsibility must be assigned for reviews of each business continuity plan. The identification
of changes in business arrangements not yet reflected in the business continuity plans must be
followed by an appropriate update of the plan. This formal change control process should ensure
that the updated plans are distributed and reinforced by regular reviews of the complete plan
(Business Continuity Review Interval).

14 Compliance

14.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of
any security requirements.

The design, operation, use, and management of information systems may be subject to statutory,
regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from legal advisers, or suitably qualified
legal practitioners. Legislative requirements vary from country to country and may vary for
information created in one country that is transmitted to another country (i.e. trans-border data
flow).

14.1.1 Identification of applicable legislation

Control: All relevant and applicable statutory, regulatory, and contractual requirements and the
approach to meet these requirements must be explicitly defined, documented, and kept up to date
for the service and the service providing organisation.
The specific controls and individual responsibilities to meet these requirements must be similarly defined and documented.

14.1.2 Intellectual property rights (IPR)

Control: Procedures must be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

The following guidelines should be considered:

a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

b) acquiring software only through known and reputable sources, to ensure that copyright is not violated;

c) maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them;

d) maintaining asset registers, and identifying all assets with requirements to protect intellectual property rights;

e) maintaining proof and evidence of ownership of licenses, master disks, manuals, etc;

f) implementing controls to ensure that any maximum number of users permitted is not exceeded;

g) carrying out checks that only authorised software and licensed products are installed;

h) providing a policy for maintaining licence conditions;

i) providing a policy for disposing or transferring software to others;

j) using appropriate audit tools;

k) complying with terms and conditions for software and information obtained from public networks;

l) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law;

m) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.
14.1.3 Protection of records

Control: Important records must be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Records must be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures, must also be stored to enable decryption of the records for the length of time the records are retained.

To meet the record safeguarding objectives, the following steps must be taken:

a) guidelines must be issued on the retention, storage, handling, and disposal of records and information;

b) a retention schedule must be drawn up identifying records and the period of time for which they should be retained;

c) an inventory of sources of key information must be maintained;

d) controls must be implemented to protect records and information from loss, destruction, and falsification.

14.1.4 Data protection and privacy of personal information

Control: Data protection and privacy must be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

A data protection and privacy policy must be developed and implemented. This policy must be communicated to all persons involved in the processing of personal information.

14.1.5 Prevention of misuse of information processing facilities

Control: Users must be deterred from using information processing facilities for unauthorised purposes.

The senior management must approve the use of information processing facilities. Any use of these facilities for non-business purposes without management approval, or for any unauthorised purposes, should be regarded as improper use of the facilities. If any unauthorised activity is identified by monitoring or other means, this activity should be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Legal advice must be taken before implementing monitoring procedures.
All users should be aware of the precise scope of their permitted access and of the monitoring in place to detect unauthorised use.

At log-on, a warning message should be presented to indicate that the information processing facility being entered is under the responsibility of the respective part of the service providing organisation and that unauthorised access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process.

14.1.6 Regulation of cryptographic controls

Control: Cryptographic controls must be used in compliance with all applicable agreements, laws, and regulations.

Legal advice must be sought to ensure compliance with national laws and regulations. Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

14.2 Compliance with security policies and technical compliance

Objective: To ensure compliance of the service with security policies and standards.

The compliance of information systems with security policies must be reviewed at least every three years and/or when significant changes occur. Such reviews must be performed against the existing security policies and the technical platforms. The service must be checked for compliance with applicable security implementation standards and documented security controls.

14.2.1 Compliance with security policies and security requirements

Control: Managers must ensure that all security procedures are carried out correctly to achieve compliance with security policies and standard based security requirements.

At planned intervals (Compliance Review Interval) and/or when significant changes occur, the compliance of information processing with the existing security policies and any other security requirements must be reviewed.

If any non-compliance is found as a result of the review:

a) determine the causes of the non-compliance;

b) evaluate the need for actions to ensure that non-compliance do not recur;

c) determine and implement appropriate corrective action;

d) review the corrective action taken.
Results of reviews and corrective actions carried out must be recorded and these records must be maintained. The results must be reported to the persons carrying out the independent reviews, when the independent review takes place.

### 14.2.2 Technical compliance checking

**Control:** Information systems must be regularly checked for compliance with the security policy and standard based security requirements.

Technical compliance checking\(^{23}\) must be performed either manually (supported by appropriate software tools, if necessary) by an experienced system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist. It must be performed on a regular basis (*Technical Compliance Check Interval*) and/or when significant technical changes occur. Such tests must be planned and documented.

Any technical compliance check must only be carried out by competent, authorised persons, or under the supervision of such persons.

### 14.3 Information systems audit considerations

**Objective:** To maximise the effectiveness of, and to minimise interference to/from the information systems audit process.

There must be controls to safeguard operational systems and audit tools during information systems audits.

Protection is also required to safeguard the integrity and prevent misuse of audit tools.

### 14.3.1 Information systems audit controls

**Control:** Audit requirements and activities involving checks on operational systems must be carefully planned and agreed to minimise the risk of disruptions to business processes.

The following points must be observed:

- a) audit requirements must be agreed with appropriate management;
- b) the scope of the checks must be agreed and controlled;
- c) the checks should be limited to read-only access to software and data;

\(^{23}\) e.g. penetration tests and/or vulnerability assessments
14.3.2 Protection of information systems audit tools

**Control:** Access to information systems audit tools must be protected to prevent any possible misuse or compromise.

Information systems audit tools, e.g. software or data files, must be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection. 

---

**d)** access other than read-only are only allowed for isolated copies of system files, which must be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

**e)** resources for performing the checks must be explicitly identified and made available;

**f)** requirements for special or additional processing should be identified and agreed;

**g)** all access must be monitored and logged to produce a reference trail;

**h)** all procedures, requirements, and responsibilities must be documented;

**i)** the person(s) carrying out the audit must be independent of the activities audited.
FRAMEWORK AGREEMENT

SCHEDULE 11
EXIT MANAGEMENT
Table of contents

1 Introduction ................................................................................................................ 1

2 Scope and General Approach of Exit Management ............................................... 2
   2.1 Scope .................................................................................................................. 2
   2.2 General approach of Exit Management ............................................................... 2
   2.3 Relation with the non-euro area NCBs ................................................................. 2

3 Exit of the Contracting CSD ..................................................................................... 3
   3.1 General responsibilities of the parties ................................................................. 3
   3.2 Responsibilities of the Contracting CSD .............................................................. 3
   3.3 Responsibilities of the Eurosystem ...................................................................... 4
Framework Agreement
Schedule 11 – Exit Management

1 Introduction

This Schedule sets out the provisions related to preparing and supporting the exit of a Contracting CSD and its community from T2S, as well as the roles and responsibilities of the parties during the exit process.

This Schedule does not cover the possible causes of termination and their consequences, nor the decision-making process, including arbitration and escalation, which will take place in case one contracting party does not accept the other contracting party’s termination of the Framework Agreement for cause.

The Schedule is divided into two chapters i) scope and general approach of the Exit Management; ii) exit of a Contracting CSD to T2S addressing the responsibilities of the parties.
2 Scope and General Approach of Exit Management

2.1 Scope

This Schedule describes the operational and mutual support principles that will apply from the moment the Contracting CSD has formally notified the Eurosystem of its decision to exit T2S, either for convenience or for cause, or from the moment the Eurosystem has formally notified the Contracting CSD that it wishes to terminate the Framework Agreement. Notifications are given by way of an official termination notice, either from the Contracting CSD to the Eurosystem, or from the Eurosystem to the CSDs.

2.2 General approach of Exit Management

Unless otherwise agreed between the parties, in writing the exit of a CSD from T2S will consist of a full de-migration of the Contracting CSD’s business on a given date (i.e. “big-bang” approach) from the T2S Platform. Such exit shall take place over a weekend, targeting to avoid sensitive weekends (e.g. end-of-month, end-of quarter).

If a CSD decides to terminate the Framework Agreement for convenience, it shall maintain its internal systems sufficiently compatible with the T2S functionality and with agreed Service Levels, so as to allow T2S to provide the agreed services to other T2S Actors. This may imply that the Contracting CSD has to implement authorised changes, in particular in case of fast-track changes, as specified in Schedule 9 (Change and Release Management).

2.3 Relation with the non-euro area NCBs

Should a non-euro area NCB terminate the Currency Participation Agreement at least six months before their planned migration date, which means that such non-euro area NCB will not migrate to T2S, the Eurosystem shall review the testing and migration plans in accordance with the provisions laid down in Schedules 2 (T2S Programme Planning and Monitoring), 3 (User Testing) and 4 (Migration).
3 Exit of the Contracting CSD

3.1 General responsibilities of the parties

a) It is the responsibility of the Eurosystem to co-ordinate, steer and monitor the exit process. In agreement with the Contracting CSD, it establishes the exit plan, the tasks and the milestones for the exit process and monitors compliance with the agreed procedures, tasks and milestones.

b) To the extent possible, the parties shall use all reasonable endeavour to minimize the effects of the exit on T2S and other T2S Actors.

c) It is the responsibility of the Contracting CSD to co-ordinate all exit activities with its T2S Users. Both parties shall appoint an “Exit Manager”, whose main responsibility consists in co-ordinating the exit activities and acting as liaison for the other contracting party.

d) The exit process ends when the adaptations are completed so that there are no more securities on the Securities Accounts managed by the CSD on the T2S Platform. Unless otherwise agreed between the parties, the exit of a CSD from T2S will take the form of a simultaneous inactivation of all Securities Accounts operated by that CSD on the T2S Platform, so as to prevent any further securities settlement on those accounts. These activities will take place during a week-end agreed upon by both parties and called the exit week-end.

After the completion of the exit process, and until the end of the legal archiving period, the Eurosystem shall continue to provide information – including but not limited to Transactional Data – to the Contracting CSD, upon the latter’s request, with respect to the services provided by the Eurosystem to the Contracting CSD in the context of the Framework Agreement.

3.2 Responsibilities of the Contracting CSD

In view of ensuring a successful exit from T2S, the Contracting CSD shall:

e) deliver to the Eurosystem, at the latest one month after the official termination notice, a high-level exit plan clearly defining all activities that – within the following conditions – the CSD itself, its DCP, the Eurosystem and, where relevant, any non-euro area NCB are to perform;

f) all its DCPs will have stopped their direct connection to T2S at least one month before the exit weekend;

g) agree with its Investor and Issuer CSD(s) how to re-arrange their inter-CSD links;

h) specify its plan to conduct tests with its Investor and Issuer CSD(s), as far as the latter remain in T2S;
Framework Agreement

Schedule 11 – Exit Management

3.2 i) agree with the Central Banks whose currency it needs for DvP settlement, how the usage of cash accounts will change as a result of the exit;

j) deliver to the Eurosystem, at the latest two months after the delivery of the high-level exit plan, the detailed support request for the execution of all exit activities, which the CSD expects from the Eurosystem;

k) monitor and take all necessary measures to facilitate the readiness of its community for the exit from T2S;

l) co-operate with the Eurosystem in preparation of the exit plan and the detailed exit weekend script;

m) coordinate all exit activities with its community, including with other CSDs acting as Investor CSDs, and confirm the successful completion of the activities to the Eurosystem;

n) inform the Eurosystem of any unexpected event or delay of a planned activity, which may affect the execution of the Eurosystem’s support activities or the exit plan.

3.3 Responsibilities of the Eurosystem

In view of ensuring a successful exit from T2S, the Eurosystem shall:

a) continue to provide all services and support as specified in the Framework Agreement, until the exit weekend;

b) provide reasonable support to the Contracting CSD in preparing its high-level exit plan;

c) indicate to the Contracting CSD within one month after the receipt of the high-level exit plan, any constraints and conditions applicable to the support it can provide;

d) assist the Contracting CSD in preparing its detailed support request to the Eurosystem, in particular by indicating specific areas where the Eurosystem can offer such support;

e) agree with the Contracting CSD within one month after the receipt of the detailed support request on the precise activities that the Eurosystem will conduct, and their timing;

f) support the Contracting CSDs in establishing the exit plan, including aspects related to its Securities Accounts, accounts structures, Dedicated Cash Accounts, major project milestones, as well as checkpoints to be met before the start of the exit weekend;

g) inform the Contracting CSD within one month after reaching an agreement on the exit plan of the amount of any costs for planning, co-ordination and execution of exit activities – beyond the normal operational support – which it expects the CSD to reimburse, unless the Contracting CSD has terminated the Framework Agreement for cause, in which case the Eurosystem will provide such support free of charge;
Framework Agreement

Schedule 11 – Exit Management

h) make all reasonable efforts to conduct the agreed activities, including communication and
coordination with other T2S Actors, and where relevant confirm their successful completion
to the Contracting CSD;

i) establish the detailed exit weekend script which provides the Contracting CSD with the
required information to execute the tasks and/or to carry out the actions required during the
exit weekend;

j) provide all reasonable support to the Contracting CSD to address any unexpected events
during the exit process;

k) establish the fall-back arrangements and roll-back procedures specific for the exit, in order to
manage the necessary processes if the exit needs to be deferred to a later stage due to
predictable or unforeseen circumstances, and/or if the activities already performed during the
exit weekend need to be unwound if the exit has to be stopped.
FRAMEWORK AGREEMENT

SCHEDULE 12
FORM FOR SUBCONTRACTING
Framework Agreement
Schedule 12 – Form for subcontracting

Name of the entity providing the services/products:
______________________________________________________________________________

Name, company number and registered office address of the entity to which the provision of services/products is subcontracted (“Subcontractor”):
______________________________________________________________________________

Detailed description of the services/products subject to Subcontracting:
______________________________________________________________________________
______________________________________________________________________________

Address from which the services/products will be provided/supplied:
______________________________________________________________________________

Contractual basis of Subcontracting (express confirmation of compliance with confidentiality and data protection obligation, right of access to the Contracting CSD premises and systems and disaster recovery):
______________________________________________________________________________

Date of initial notification of Subcontracting: _________________________________________

Form of the notification of Subcontracting:  __________________________________________

Action required:
The CSG shall respond within 14 calendar days from receipt of the request of consent and decide in alternative to:

(i) provide its consent
(ii) refuse its consent

In case of (ii) reasons for refusal: _____________________________________________

(iii) indicate a new deadline for providing the answer (not later than 1 month from receipt of the Eurosystem’s request):
______________________________________________________________________________

Authorised signatories
Eurosystem
For consent, _______________________________________________________  ______________________
Contracting CSD/CSG
Authorised signatories
FRAMEWORK AGREEMENT

SCHEDULE 13

PROCEDURE FOR PAYMENT OF CLAIMS
Framework Agreement

Schedule 13 – Procedure for payment of claims

Table of contents

1 Procedure in respect of claims pursuant to Articles 32 and 33(1)(b) .................1
2 Procedure in respect of claims pursuant to Article 40........................................3
3 Procedure in respect of claims pursuant to Articles 21(7) and 33(1)(a)..........5
4 Procedure in respect of claims pursuant to Article 28(4)...............................7
For the purposes of this Schedule, either Party asserting a claim against the other Party is referred to as “Claimant”, while the other Party is referred to as “Respondent”.

1 Procedure in respect of claims pursuant to Articles 32 and 33(1)(b)

The following procedure applies to the handling of any claim pursuant to Articles 32 or 33(1)(b):

(a) The Claimant shall notify the Respondent without undue delay of the occurrence of any event which the Claimant reasonably believes may give rise to a claim for liability or indemnification, as the case may be, and in any case no later than within 30 calendar days from the occurrence of such an event or, if the Claimant did not know that an event would give rise to a claim, as from the moment it has the relevant knowledge.

(b) The Claimant shall submit its claim against the Respondent without undue delay, and in any case no later than within 12 months from the occurrence of the event which gave rise to the claim or, if the Claimant did not know that an event gave rise to a claim for liability or indemnification, within 12 months from the moment it knew or should reasonably have known of such a claim. After the expiry of this period, the Respondent shall be entitled to reject the claim.

(c) The Claimant shall submit its claim to the Respondent in writing, hereby specifying the amount and justification of the claim, to allow the Respondent to assess the merits of the submitted claim.

(d) The Respondent may request any additional information from the Claimant as may be reasonably required for assessing the merits of the claim. The Claimant shall cooperate in good faith and in a timely manner with the Respondent.

(e) The Respondent shall, without undue delay, notify the Claimant in writing if it accepts the claim or rejects it in whole or in part, in the latter case giving reasons for the rejection.

(f) In case of dispute as to the merits of the claim, the Parties shall make any effort to find an amicable arrangement. As the case may be, the Parties shall take recourse to Article 43 (Arbitration).

(g) If the Respondent has accepted the claim as merited, in whole or in part, or if it was settled either by an amicable arrangement between the Parties or through an Arbitration pursuant to Article 43, the Respondent shall, subject to paragraphs (b), (h) and (i), pay out the claim as soon as reasonably practicable and at the latest within 90 calendar days after the end of the calendar year in which the event occurred that caused the claim. Any payment pursuant to Article 32 is subject to the limitations of Article 32(5)(a) and shall be made on a provisional basis subject to the reservations of paragraphs (h) and (i). The Claimant shall
Framework Agreement

Schedule 13 – Procedure for payment of claims

not be entitled to claim interest or damages for late payment in relation to the time elapsed prior to the expiry of the period of 90 calendar days.

(h) If the liability of the Eurosystem vis-à-vis the Contracting CSD is limited in accordance with Article 32(5)(a) and the amounts payable to the Contracting CSD and, as the case may be, to other Participating CSDs are reduced accordingly, the Eurosystem shall notify all Claimants as soon as practicably possible after the end of the calendar year referred to in paragraph (g); the notification shall give sufficient evidence of the reasons for, and the calculation of, the reduced amounts paid in relation to the amounts that had been claimed.

(i) If a claim is accepted as merited by the Eurosystem after the end of the calendar year in which the event occurred that caused the claim or settled either by an amicable arrangement between the Parties or through an Arbitration pursuant to Article 43 after the end of this calendar year, the Eurosystem shall pay such a claim as soon as reasonably practicable. If such a claim should be subject to a reduction pursuant to Article 32(5)(a), the Claimant shall be notified in accordance with paragraph (h) prior to the payment. To the extent that a claim paid after the end of the calendar year referred to in paragraph (g) is subject to a reduction pursuant to Article 32(5)(a), all payments previously made to the Contracting CSD or Participating CSDs with regard to this calendar year shall be recalculated in accordance with Article 32(5)(a) and the paid amounts shall be adjusted. With regard to this adjustment, the Eurosystem is entitled to claim back any payment made in excess of the adjusted pro rata entitlement according to Article 32(5)(a).
2 Procedure in respect of claims pursuant to Article 40

The following procedure applies to the handling of claims pursuant to Article 40:

(a) The Claimant shall without undue delay, and in any case within a maximum period of 12 months after the date at which the termination of the Agreement became effective, submit the claim to the Respondent in writing, hereby specifying the amount and justification of the claim, to allow the Respondent to assess the merits of the claim. After the expiry of this maximum period, the Respondent shall be entitled to reject the claim.

(b) The Respondent may request any additional information from the Claimant as may be reasonably required for assessing the merits of the submitted claim. The Claimant shall cooperate in good faith and in a timely manner with any such requests by the Respondent.

(c) The Respondent shall, without undue delay, notify the Claimant in writing if it accepts the claim or rejects it in whole or in part, in the latter case giving reasons for the rejection.

(d) In case of dispute as to the merits of the claim, the Parties shall take recourse to Article 42 and, as the case may be, Article 43.

(e) The Respondent shall compensate any claim that it has accepted as merited, in whole or in part, or that was settled in accordance with Articles 42 or 43, as soon as reasonably practicable and at the latest within 90 calendar days after the end of the calendar year in which the claim was accepted or settled. The Claimant shall not be entitled to claim interest or damages for late payment in relation to the time elapsed prior to the expiry of the period of 90 calendar days.

(f) The following shall apply in respect of the calculation of the loss payable by the Contracting CSD to the Eurosystem, in accordance with Article 40(1):

- The loss shall be calculated as from the date when the termination of the Agreement became effective.

- It shall be calculated as follows: “daily average number of securities instructions that the Contracting CSD settled, as the case may be, either in T2S or in its legacy settlement infrastructure during the 12 month preceding the date of notification of termination multiplied by the relevant T2S prices indicated in the T2S Price List multiplied by the number of days from the date when the termination became effective until the end of the cost recovery period”.

(g) The following shall apply in respect of the calculation of any Direct Loss payable by the Eurosystem to the Contracting CSD, in accordance with Article 40(2) of this Agreement:
The Contracting CSD shall be entitled to claim compensation for the Direct Loss it suffered as a result of the Eurosystem’s termination.

Such Direct Loss shall be calculated as from the date when the termination of the Agreement became effective and shall cover (1) a maximum period of 24 months, or, (2) the time until the end of the T2S cost recovery period, whichever of (1) or (2) is the shorter period.

To the extent the Contracting CSD’s Direct Loss relates to interest on its T2S related investments made, the amount of such interest shall be determined as follows: “amount of T2S related investment multiplied by the number of days multiplied by the ECB Main Refinancing Rate (as applicable during the period for which the Eurosystem has to pay compensation)”.

The Direct Loss that the Eurosystem has to pay shall be limited to the equivalent of the T2S fees that the Contracting CSD could be reasonably expected to pay during the period of 24 months after the date when the termination of the Agreement became effective. The Contracting CSD’s expected T2S fees shall be determined as follows: “daily average number of securities instructions that the Contracting CSD settled, as the case may be, either in T2S or in its legacy settlement infrastructure during the 12 month preceding the date of notification of termination multiplied by the relevant T2S prices indicated in the T2S Price List multiplied by the number of days the Eurosystem has to pay compensation (max. 24 months from the date when the termination became effective, but no longer than until the end of the cost recovery period)”.

3 Procedure in respect of claims pursuant to Articles 21(7) and 33(1)(a)

The following procedure applies in addition to Articles 21(7) and 33(1)(a) if legal action is commenced or threatened against the Eurosystem:

(a) If the Eurosystem allows the Contracting CSD to control the defense against the Third Party claimant, the Contracting CSD shall keep the Eurosystem informed of all material matters at all times. Notwithstanding such agreement regarding the control over the defense, the Eurosystem, being the formal party to the legal proceedings, and the Contracting CSD shall agree on the way in which the proceedings are conducted. For this purpose, and in due consideration of the agreement to give the Contracting CSD control over the defense, the Eurosystem shall be entitled to object to legal submissions proposed by the Contracting CSD that it considers harmful to the outcome of such proceedings and to make its own counter proposals towards the Contracting CSD. Expenses of the Eurosystem in the context of such involvement shall be borne by the Eurosystem.

(b) At the request of the Contracting CSD the Eurosystem shall give all reasonable assistance and provide all relevant documents and data which are under its control, to the extent permissible under the applicable statutory and contractual law. The Contracting CSD shall indemnify the Eurosystem for all reasonable cost the latter incurred in that context.

The following procedure applies in addition to Articles 21(7) and 33(1)(a) if the Eurosystem is held legally liable to the Third Party:

(c) The Eurosystem shall notify the Contracting CSD of the fact that it is held liable to the Third Party pursuant to an Enforceable Judgment. The notification shall be sent as soon as reasonably practicable but in no case later than 30 days after the full text of the Enforceable Judgment was available to the Eurosystem.

(d) The notification shall contain a statement to the effect that the Eurosystem intends to claim reimbursement from the Contracting CSD, the text of the Enforceable Judgment (to the extent available) and a preliminary indication of the amount and composition of the claim.

(e) The Eurosystem shall submit its claim to the Contracting CSD in writing and without undue delay and in any case no later than 90 calendar days after the full text of the Enforceable Judgment was made available to the Eurosystem. A delay shall not relieve the Contracting CSD of its obligation to reimburse the Eurosystem, except to the extent that the Contracting CSD can demonstrate that the delay caused damages.

(f) The Eurosystem shall precisely set out the amount and the various components of the payment it owes to the Third Party and for which it claims reimbursement from the
Contracting CSD. The Contracting CSD may request any additional information from the Eurosyste
The Eurosystem shall cooperate in good faith with any such request by the Contracting CSD.
(g) The Contracting CSD shall notify the Eurosystem in writing within 90 calendar days from the day of the receipt of the claim if it accepts the claim or rejects it in whole or in part, in the latter case giving reasons for the rejection.
(h) In case of dispute as to the merits of the claim, the Parties shall take recourse to Article 43 (Arbitration).
(i) The Eurosystem shall subrogate the Contracting CSD to any rights it may have against Third Parties in relation to the reimbursed claim.
4 Procedure in respect of claims pursuant to Article 28(4)

The following procedure applies in addition to Article 28(4) if legal action is commenced or threatened against the Contracting CSD:

(a) If the Contracting CSD allows the Eurosystem to control the defense against the Third Party claimant, the Eurosystem shall keep the Contracting CSD informed in all material matters at all times. Notwithstanding such agreement regarding the control over the defense, the Contracting CSD, being the formal party to the legal proceedings, and the Eurosystem shall agree on the way in which the proceedings are conducted. For this purpose, and in due consideration of the agreement to give the Eurosystem control over the defense, the Contracting CSD shall be entitled to object to legal submissions proposed by the Eurosystem that it considers harmful to the outcome of such proceedings and to make its own counter proposals towards the Eurosystem. Expenses of the Contracting CSD in the context of such involvement shall be borne by the Contracting CSD.

(b) At the request of the Eurosystem the Contracting CSD shall give all reasonable assistance and provide all relevant documents and data which are under its control, to the extent permissible under the applicable statutory and contractual law. The Eurosystem shall indemnify the Contracting CSD for all reasonable cost the latter incurred in that context.

The following procedure applies in addition to Article 28.4(b) if the Contracting CSD is held legally liable to the Third Party:

(c) The Contracting CSD shall notify the Eurosystem of the fact that it is held liable to the Third Party pursuant to an Enforceable Judgment. The notification shall be sent as soon as reasonably practicable but in no case later than 30 days after the full text of the Enforceable Judgment was available to the Contracting CSD.

(d) The notification shall contain a statement to the effect that the Contracting CSD intends to claim reimbursement from the Eurosystem, the text of the Enforceable Judgment (to the extent available) and a preliminary indication of the amount and composition of the claim.

(e) The Contracting CSD shall submit its claim to the Eurosystem in writing and without undue delay and in any case no later than 90 calendar days after the full text of the Enforceable Judgment was made available to the Contracting CSD. A delay shall not relieve the Eurosystem of its obligation to reimburse the Contracting CSD, except to the extent that the Eurosystem can demonstrate that the delay caused damages.

(f) The Contracting CSD shall precisely set out the amount and the various components of the payment it owes to the Third Party and for which it claims reimbursement from the
Framework Agreement
Schedule 13 – Procedure for payment of claims

188 Europsystem. The Eurosystem may request any additional information from the Contracting
189 CSD as may be reasonably required for assessing the merits of the submitted claim. The
190 Contracting CSD shall cooperate in good faith with any such request by the Eurosystem.
191 (g) The Eurosystem shall notify the Contracting CSD in writing within 90 calendar days from
192 the day of the receipt of the claim if it accepts the claim or rejects it in whole or in part, in
193 the latter case giving reasons for the rejection.
194 (h) In case of dispute as to the merits of the claim, the Parties shall take recourse to Article 43
195 (Arbitration).
196 (i) The Contracting CSD shall subrogate the Eurosystem to any rights it may have against
197 Third Parties in relation to the reimbursed claim.