EUROPEAN CENTRAL BANK

EUROSYSTEM

Eurosystem report on the gap assessment of card payment schemes against the "Oversight framework for card payment schemes – standards"

1 Executive summary

On 4 January 2008 the Governing Council of the European Central Bank (ECB) approved the "Oversight framework for card payment schemes – standards", which lays down the Eurosystem oversight requirements for card payment schemes (CPSs) operating in the euro area. The aim of these standards is to promote the reliability of CPSs operating in the euro area, public confidence in card payments and a level playing field in the domain of card payments across the euro area. Following the publication of the above framework, in May 2008 the Eurosystem started implementing the harmonised oversight of the CPSs operating in the euro area. 23 CPSs were assessed against the standards and the findings of that assessment were summarised in the 2014 Eurosystem oversight report[1]. The vast majority of oversight recommendations stemming from the above assessment exercise have in the meantime been comprehensively addressed by the overseen schemes and the follow-up measures were considered satisfactory by the overseers. A few remaining recommendations (for two schemes only) are still being followed up by the schemes in dialogue with the overseers and are mentioned in Section 3 of this report, together with the findings of the latest assessment.

An updated version of the "Guide for the assessment of card payment schemes against the oversight standards" was published in February 2015, taking into account

[1] Eurosystem oversight report 2014, pp. 27-28.

the “SecuRe Pay Recommendations on the security of internet payments” (which were later, with some deviations, adopted as European Banking Authority (EBA) Guidelines). The assessment guide translates the applicable standards into more detailed oversight requirements and thereby supports a comprehensive and efficient assessment against these standards. Following the publication of the updated assessment guide, the Eurosystem decided to conduct a **“gap assessment”** focusing only on the differences between the original and the updated assessment guide. **This Eurosystem report provides an overview of the gap assessments of 16 CPSs against the Eurosystem standards, covering 13 national CPSs[2] and 3 international CPSs operating in the euro area, with consideration being given to the observance rating assigned in the previous comprehensive assessment and the follow-up thereto, and presents an overview of the observance levels for all applicable oversight requirements.** Some schemes have not been assessed as they are subject to a waiver defined in the standards. This waiver exempts from the oversight requirements the schemes under which less than one million cards are issued per year on average over three years or having average transactional values of less than €1 billion over three years. The Eurosystem gap assessment exercise was conducted sequentially starting in the second quarter of 2015 and was finalised in the third quarter of 2018.

This report describes the main findings and the final oversight conclusions concerning the observance of assessed CPSs of the oversight standards. The implementation of the recommendations is closely monitored by the overseers.

The Eurosystem concluded that of the 16 CPSs, 11 fully observe all oversight standards and the remaining 5 broadly observe the standards.

Almost all CPSs were assessed as fully observing aspects covering the soundness of the scheme’s legal basis (standard 1), where the main focus of the gap assessment was on the adaptations of the scheme rules to recent changes in relevant EU legislation. All schemes demonstrated that they had dedicated adequate attention to continued compliance with regulatory requirements, although only a few schemes have ongoing processes in place to ensure full compliance.

A similar positive assessment has been made with respect to the schemes’ rules on access to comprehensive information (standard 2), with the majority of schemes fully observing the standard.

Despite the fact that overall observance levels were lowest for security, operational reliability and business continuity issues (standard 3), it is highlighted that at the level of key issues only seven schemes were found to have some deficiencies. The most significant findings in this gap assessment were made in the area of security risk management (key issue 3.1) and transactions (3.3). Negatively assessed aspects mainly related to the evaluation of devices and customer authentication procedures by competent third parties and the management of so-called secrets (e.g. safeguarding the security credentials or cryptographic material). Furthermore, some

[2] Down from 16 during the course of the assessment due to mergers and acquisitions.

CPSs did not impose an obligation on their service providers to conduct their own risk analyses in line with the scheme rules. Finally, for a few schemes the security features for the secure authentication of the card holder in remote electronic transactions were not always sufficiently defined. On a more positive note, however, many schemes have already put in place efficient measures to monitor all transactions processed and block potentially fraudulent transactions.

For governance arrangements (standard 4), almost all CPSs were assessed as fully observing the standard. For standard 5, focusing on the clearing and settlement process, all schemes were found to be fully compliant, with only very minor deficiencies at the level of key issues.

2 Background information on the oversight assessment

The "Oversight framework for card payment schemes – standards", as approved by the Governing Council of the ECB on 4 January 2008, applies to all card payment schemes. This includes three-party and four-party CPSs providing card payment services for debit and/or credit cards. For the purpose of the oversight framework, a CPS is defined as the set of functions, procedures, arrangements, rules and devices that enable a holder of a payment card to effect a payment and/or cash withdrawal transaction with a third party other than the card issuer. The standards of the framework are addressed to the governance authority (GA) of the CPS, i.e. the authority which is responsible for ensuring compliance. However, in agreement with the overseer, the GA may have appointed another actor/other actors to be responsible for certain CPS functions. In such cases, the boundaries with respect to the individual responsibilities of the various actors must be clearly defined, transparent and documented.

A waiver policy was applied in order to allocate oversight efforts proportionally to the risks created by the schemes, and to prevent overburdening small CPSs. The requirement to participate in this gap assessment could have been waived for CPSs which, within the euro area and over the past three years, had: (1) an annual average sum of cards-in-issue of less than 1 million; or (2) an annual average value of transactions of less than €1 billion.[3] However, in a number of cases, national overseers nevertheless decided to assess schemes to which the waiver could have been applied.

The oversight framework for CPSs is based on a risk-based approach covering different areas of risk independently to ensure that all of the relevant risks to which card schemes are exposed are properly addressed. These considerations have led to the establishment of five standards against which compliance is assessed. In short, each CPS should:

1 have a sound legal basis under all relevant jurisdictions;

[3] As defined in the "Oversight framework for card payment schemes – standards" as criteria exempting a scheme from the application of the oversight requirements defined therein.

2 ensure that comprehensive information, including appropriate information on financial risks, is available to the actors;

3 ensure an adequate degree of security, operational reliability and business continuity;

4 have effective, accountable and transparent governance arrangements;

5 manage and contain financial risks in relation to the clearing and settlement process.

Each of these five standards consists of a number of sub-domains with key issues defining more detailed oversight requirements under each standard (see Annex 1 for an overview).

To conduct the gap assessment, the common assessment guide for all overseen CPSs with concrete assessment questions (AQs) and check-points was developed for each of the key issues and updated in 2015, as described in Section 1. This amended assessment guide aimed to foster a common understanding of the oversight standards among overseers and by CPSs and to ensure consistency of the assessments across all CPSs with their different business features as well as different governance structures.[4] As the **first step** in the assessment process, the AQs were answered by the respective GA of the CPSs. The answers to the questions were accompanied by a justification and reference supporting documentation.

The **second step** in the assessment process consisted of a review of the answers of the CPSs by the overseers, leading to a conclusion on the degree of compliance by the lead overseer per question (Yes/No/Not applicable), and per respective key issue (observed, broadly observed, partly observed, not observed). International card schemes were assessed following a cooperative oversight approach whereby an Assessment Group of experts from several central banks collaborated in drafting the assessment.

Based on the findings established in the previous steps, the **third step** consisted in developing recommendations to address shortcomings in terms of the observance of oversight requirements. Such findings and related recommendations were discussed with the respective CPSs and concrete follow-up actions have been/are being agreed. In some cases, improvements have already been put in place and have been assessed by the overseer during the course of the assessments, and the observance levels have been adjusted accordingly.

In the **fourth step**, the draft assessments of domestic CPSs were peer-reviewed in order to cross-check the assessment reports by independent overseers (representing national central banks other than the lead overseer), with the purpose of further enhancing consistency and comparability of the assessment of all CPSs.

[4] These differences have also been considered and addressed, where relevant, in the oversight assessment.

For international CPSs, the peer reviews took place within the Assessment Group, with each member having reviewed the full report.

3 Observance status

3.1 Observance at the level of the standards

This section of the report provides an overview of the assessments of the 16 CPSs against the Eurosystem standards (see the table in Annex 1 for a full list of applicable key issues), covering 3 international card payment schemes[5] and 13 national card payment schemes[6] operating in the euro area which are not subject to a waiver. Schemes operating at national level are usually co-branded with an international scheme, mainly – but not only – in order to enable the processing of cross-border transactions. Table 1 below summarises the assessment of compliance at the most aggregated level of the standards.

Table 1
Observance levels per oversight standard

	1. legal basis	2. comprehensive information	3. security, operational reliability & business continuity	4. governance arrangements	5. clearing & settlement process
Observed	15	13	13	14	16
Broadly observed	1	3	3	2	0
Partly observed	0	0	0	0	0
Not observed	0	0	0	0	0
Not applicable	0	0	0	0	0

The table above indicates that almost all CPSs are fully/broadly observing the oversight standards (see the following sections for a detailed evaluation). 11 CPSs observe all applicable standards. In comparison with the previous (2014) comprehensive assessment exercise, the tables above present an overall higher level of compliance with the oversight standards, which indicates increased attention of the overseen CPSs to risk management and the further development of their compliance functions. In the following sub-sections, the observance of the specific standards is presented in more detail, including some findings and recommendations resulting from the assessment which are common to a number of schemes.

5 Providing services on a euro area-wide scale.

6 Down from 16 during the course of the assessment due to mergers and acquisitions.

3.1.1 Standard 1 - a CPS should have a sound legal basis under all relevant jurisdictions

The first standard consists of two key issues:

- (1.1) the legal framework governing the establishment and functioning of a CPS and the relationship between the CPS and its issuers, acquirers, customers and service providers should be complete, unambiguous, up-to-date, enforceable and compliant with the applicable legislation; and
- (1.2) where different jurisdictions govern the operation of the scheme, the law of those jurisdictions should be analysed in order to identify the existence of any conflicts. Where such conflicts exist, appropriate arrangements should be made to mitigate the consequences of such conflicts.

Since there were no changes of substance in the revised assessment guide for standard 1, the assessment focus was on the plans and actions of individual CPSs to ensure compliance with the recent relevant legislation (e.g. revised Payment Services Directive[7], Anti-Money Laundering Directive[8] and Interchange Fees Regulation[9]).

Table 2 below provides an overview of the ratings of all CPSs.

Table 2

Observance levels for key issues under standard 1[10]

	1.1 legal framework	1.2 conflicting jurisdictions
Observed	15	9
Broadly observed	1	0
Partly observed	0	0
Not observed	0	0
Not applicable	0	7

All but one CPS fully observed the standard. With regard to relevant regulatory developments, the schemes demonstrated to the overseers that dedicated measures have been put in place to assess the impact of the respective regulations on the functioning of the schemes. This process was often driven by the general review clauses in the scheme rules, which include a major change in applicable legislation as a trigger for the rules' review. For national schemes not offering cross-border facilities, the second key issue is not applicable (seven cases).

7 Directive (EU) 2015/2366 on payment services in the internal market (PSD2).

8 Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC.

9 Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions.

10 Key issue 1.2 is not applicable to schemes which only operate in a single jurisdiction.

3.1.2 Standard 2 - a CPS should ensure that comprehensive information, including appropriate information on financial risks, is available to the actors

The second standard consists of two key issues:

- (2.1) requires that all rules and contractual arrangements governing the CPS should be adequately documented and kept up-to-date. All actors and potential actors should be able to easily access information relevant to them, to the extent permitted by the relevant data protection legislation, so that they can take appropriate action in all circumstances. Sensitive information should only be disclosed on a need-to-know basis; and
- (2.2) covers the access to information: issuers, acquirers, card holders and card acceptors should have access to relevant information in order to evaluate financial risks affecting them.

In the revised assessment guide, greater emphasis has been put on the communication with all actors, in particular with respect to complaint reporting, security awareness, fraud and charge-backs. Moreover, the information that has to be provided to card holders and merchants' has been expanded to cover more comprehensively the security and financial risks related to the participation in the scheme. Table 3 below provides an overview of the ratings of all CPSs.

Table 3

Observance levels for key issues under standard 2

	2.1 governance adequately documented	2.2 access to information
Observed	16	13
Broadly observed	0	1
Partly observed	0	2
Not observed	0	0
Not applicable	0	0

Current compliance with standard 2 is good, with all CPSs being fully compliant with key issue 2.1 and most schemes with key issue 2.2. Given the high level of compliance, there were only a few recommendations for some CPSs in the initial assessments. The only areas for improvement which resulted in recommendations for some CPSs were related to the obligations set out by the CPSs for their card issuers and acquirers to inform card holders (payers) and card acceptors (payees) about the security and financial risks connected with their participation in the scheme.

3.1.3 Standard 3 - a CPS should ensure an adequate degree of security, operational reliability and business continuity

Standard 3 is the most comprehensive standard, dealing with security, operational reliability and business continuity. This standard comprises six key issues, addressing security management (3.1), the manufacture and distribution of cards and of accepting and other technical devices (3.2), transactions (3.3), clearing and settlement (3.4), business continuity (3.5) and, finally, outsourcing (3.6).

Key issues 3.1, 3.2 and 3.3 were those where most additional requirements were added in the latest update of the assessment guide and therefore where most effort was required by the schemes to achieve and/or demonstrate compliance.

With regard to security management (key issue 3.1), more detailed requirements were added for the content and review of the security policy. These were related e.g. to the objectives and organisation of information security, roles and responsibilities, the risk assessment, and the involvement of and reporting lines of the risk management function. In addition, more detailed security requirements have been set for IT development, production and testing. Finally, the requirements for the protection of sensitive payment data and the requirements for strong customer authentication (SCA) have also been made more specific.

Concerning the manufacture and distribution of cards (3.2), authentication procedures as well as further requirements and procedures (e.g. password policy, proper definition of security features) were specified. These include the secure provision of authentication tools and the delivery of payment-related software.

The changes regarding transactions (3.3) aim to enhance the security of transactions, in particular for online transactions. These include an automatic termination of inactive payment services, as well as the introduction of risk-minimising measures for card holders (e.g. to disable the internet payment functionality, to manage limits for their cards) and for payment service providers (e.g. to suspend access to the payment service or to disable the use of cards). Table 4 below provides an overview of the ratings of all CPSs.

Table 4

Observance levels for key issues under standard 3

	3.1 security management	3.2 manufacture and distribution	3.3 transactions	3.4 clearing & settlement	3.5 business continuity	3.6 outsourcing
Observed	12	14	12	16	15	15
Broadly observed	4	2	4	0	0	0
Partly observed	0	0	0	0	1	1
Not observed	0	0	0	0	0	0
Not applicable	0	0	0	0	0	0

With respect to key issue 3.1, the majority of CPSs are compliant with the oversight requirements and only limited scope for improvement was identified for four CPSs.

One of the common issues detected was the lack of an explicit definition of sensitive payment data in the scheme rules. However, given that most card schemes have already implemented the security requirements set out by the self-regulatory body (the Payment Card Industry Standards Setting Council's Data Security Standards), the CPSs usually defined their own categories of protected information related to card holders and their personalised security credentials: Personally Identifiable Information (PII) and Account Data. In the course of the gap assessment, the overseers agreed that these data categories could be used as an approximation of the sensitive payment data. It was also found that for most schemes these data categories were adequately protected under the scheme rules. Some room for improvement has also been identified under key issue 3.1 in relation to the procedures to be followed in the event of security-related customer complaints and incidents and has been addressed in the oversight recommendations.

Given the additional focus of the gap assessment on governance of security risk management, some recommendations were related to the CPSs' internal risk analyses and security policies. These recommendations concerned the content and maintenance of such risk analyses/policies, also underlining that the requirements for the analyses/policies should be uniformly applied across a CPS (including its service providers where applicable).

With respect to the manufacturing and distribution of cards and devices (key issue 3.2), the overall compliance levels were more satisfactory, with 14 schemes being fully compliant. Some deficiencies were however identified, mainly related to the evaluation of devices and customer authentication procedures by competent third parties and the management of secrets. It is noted that in this particular area some schemes did not impose in their rules a general obligation on members to secure remote payment transactions with SCA or prescribe the mandatory set of tools related to the SCA procedure. Some schemes justified this choice by limited fraud rates and by putting alternative measures in place to address the fraud risks, e.g. active real-time monitoring of all transactions, while others demonstrated that they offer active support for their members to implement solutions offered by the scheme and incentives to apply them (e.g. liability shift rules).

On a general note, the overseers also considered that the general obligation for the payment service providers to apply SCA in card-not-present transactions has been in place in most Member States since August 2015[11]. The alternative measures described above were covered under exemptions to the above regulatory regime. Therefore, these measures were considered satisfactory to control fraud risk.

Key issue 3.3, which covers transaction-related security aspects, was found to be observed for 12 schemes, 4 schemes broadly observed this key issue. The main findings relate to insufficiently defined security features for internet payments (e.g. time-out periods, failed authentication attempts limit). There were only a few

[11] When the EBA Guidelines for the security of internet payments (EBA/GL/2014/12_Rev1) entered into force.

findings related to fraud monitoring by the scheme members (e.g. related to their reporting obligations to the GA).

Aspects related to business continuity (key issue 3.5) and the outsourcing process (key issue 3.6) were not fully observed because of shortcomings identified in the previous comprehensive assessment which have not yet been fully resolved.

3.1.4 Standard 4 - a CPS should have effective, accountable and transparent governance arrangements

Standard 4 consists of two key issues:

- (4.1) states that effective, efficient and transparent processes should be defined and implemented when making decisions about business objectives and policies, including access policies on issuers and acquirers; reviewing performance, usability and convenience of the CPS; and identifying, mitigating and reporting significant risks to its business; and
- (4.2) requires the existence of an effective internal control framework, including an adequate audit function.

The revision of the assessment guide aimed to clarify that the outcome of the customer satisfaction evaluations should be reported to the Board of the GA and that there needs to be rules for termination of the scheme membership. Moreover, an obligation for acquirers to regularly monitor card acceptors handling sensitive payment data has been introduced. Table 5 below provides an overview of the ratings of all CPSs.

Table 5
Observance levels for key issues under standard 4

	4.1 decision processes	4.2 internal control framework
Observed	15	15
Broadly observed	1	0
Partly observed	0	1
Not observed	0	0
Not applicable	0	0

Standard 4 has been very positively assessed, which indicates that almost all CPSs have effective, accountable and transparent governance arrangements, with only one scheme being broadly compliant with key issue 4.1 and one scheme being partly compliant with key issue 4.2. A positive development noted under the first key issue was the efficient processes put in place by all CPSs to analyse the performance, usability and convenience of the services offered to customers by the CPS (including procedures to report irregular, potentially fraudulent activities).

Table 5 also indicates that room for improvement was identified on the internal control framework (key issue 4.2) related to open issues identified in the previous comprehensive assessment.

3.1.5 Standard 5 - a CPS should manage and contain financial risks in relation to the clearing and settlement process

The fifth standard concerns the financial risks in relation to the clearing and settlement process. CPSs should have an overview of the risks inherent in the clearing and settlement process (5.1); the risks related to providers of clearing and settlement services (5.2); and the risks related to potential failure of the actors involved in the transactions – including awareness of such obligations (5.3), which only applies if the scheme has arrangements to complete settlement in the event of an issuer defaulting on its obligations and hence is typically not applicable to three-party schemes.

The changes introduced to standard 5 in the revision of the assessment guide were mostly editorial, introducing a differentiation between clearing and settlement arrangements. Table 6 below provides an overview of the ratings of all CPSs.

Table 6
Observance levels for key issues under standard 5

	5.1 risks	5.2 providers	5.3 actor solidity
Observed	14	16	8
Broadly observed	1	0	0
Partly observed	0	0	0
Not observed	0	0	0
Not applicable	1	0	8

Given the weighted scoring of the key issues as prescribed by the oversight framework, all schemes were assessed as observing standard 5 (where applicable). The limited number of outstanding recommendations is currently being addressed by the schemes. Therefore, while the overseers continue to monitor the follow-up actions being implemented by the GA, the ratings for the key issues in question have not been downgraded due to the limited impact on the overall scheme security.

4 General conclusions and follow-up

The main conclusion of this CPS gap assessment is that all of the assessed CPSs at least broadly observe all five standards. In comparison to the previous comprehensive assessment exercise, more schemes (11 out of 16) have achieved full compliance with all applicable standards.[12] This indicates ongoing improvements

[12] In the 2014 comprehensive assessment exercise, only 9 out of the 20 assessed schemes were found to be fully compliant with all oversight standards.

in the CPSs' risk management and internal compliance functions. Many recent changes of the CPS rules have also been driven by the increasing "bottom-up" demand of the CPSs' members for the GA's support to ensure compliance with the recent regulatory changes – the PSD2 and related secondary legislation being the most prominent example.

However, some room for improvement still exists for various aspects of risk management (especially in the area of security and fraud risks). Most notably, the assessment rules and processes related to security, operational reliability or business continuity showed insufficient results for 43% of the CPSs. Some issues as indicated above were also identified for risk-mitigation measures in the transaction phase. On a more positive note, a broad roll-out of SCA solutions for remote electronic payments has been observed for most of the schemes (where applicable, since not all schemes offer remote payments) and while not all schemes explicitly mandate the use of SCA in all transactions, it is noted that this will become mandatory as of 14 September 2019, when the RTS on SCA and CSC[13], as well as national provisions transposing Article 97 of the PSD2, become fully applicable.

As a direct result of the CPS assessment exercise, concrete recommendations were issued and, in many cases, recommendations have already been implemented or are in the course of being implemented by the CPSs. In all cases where areas for improvement persist, the overseers have scheduled follow-up actions to track the progress in addressing recommendations.

In addition to reviewing any pending follow-up actions taken by the CPSs, the overseers will continue to assess forthcoming changes within the CPSs and monitor the major security and operational incidents reported by the schemes. These activities also form part of the overseers' continuous dialogue with the overseen CPSs.

[13] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (OJ L 69, 13.3.2018, p. 23).

5 Annex
Overview of the standards and key issues

1 The CPS should have a sound legal basis under all relevant jurisdictions.

1.1 The legal framework governing the establishment and functioning of a CPS and the relationship between the CPS and its issuers, acquirers, customers and service providers should be complete, unambiguous, up-to-date, enforceable and compliant with the applicable legislation.

1.2 Where different jurisdictions govern the operation of the scheme, the law of those jurisdictions should be analysed in order to identify the existence of any conflicts. Where such conflicts exist, appropriate arrangements should be made to mitigate the consequences of such conflicts.*

2 The CPS should ensure that comprehensive information, including appropriate information on financial risks, is available to the actors.

2.1 All rules and contractual arrangements governing the CPS should be adequately documented and kept up-to-date. All actors and potential actors should be able to easily access information relevant to them, to the extent permitted by the relevant data protection legislation, so that they can take appropriate action in all circumstances. Sensitive information should only be disclosed on a need-to-know basis.

2.2 Issuers, acquirers, card holders and card acceptors should have access to relevant information in order to evaluate financial risks affecting them.

3 The CPS should ensure an adequate degree of security, operational reliability and business continuity.

3.1 Security management

3.1.1 An analysis of operational and security risks should be conducted on a regular basis in order to determine the acceptable risk level and select adequate security policies and appropriate procedures in order to prevent, detect, contain and correct security violations. Compliance with such security policies should be assessed on a regular basis.

3.1.2 Management and staff should be trustworthy and fully competent (in terms of skills, training and number of staff) to make appropriate decisions to endorse security policies and carry out their CPS-related responsibilities and duties.

* Outside of the scope of the "gap assessment".

3.1.3 Operational and incident management should be clearly defined and effectively implemented.

3.1.4 The CPS security policy should ensure privacy, integrity and authenticity of data and confidentiality of secrets (e.g. PIN) when data are operated, stored and exchanged. If secrets are revealed or compromised, effective contingency plans should be implemented to protect the CPS.

3.2 Manufacture and distribution of cards and of accepting and other technical devices

3.2.1 The design and manufacture of payment cards and of accepting and other technical devices should ensure an adequate degree of security in line with the security policies of the CPS.

3.2.2 Effective and secure procedures should be in place for the initialisation, personalisation and delivery both of cards to holders and of accepting devices to acceptors, and for the generation and delivery of secrets (e.g. PIN).

3.3 Transactions

3.3.1 Adequate security standards should be in force for the initiation of transactions in accordance with CPS security policies. CPS components should be protected from unauthorised activity. The CPS should have the capability to mitigate the risks stemming from the use of payment cards without online authorisation or with less secure authentication measures (e.g. remote payments).

3.3.2 The activities of card holders and card acceptors should be permanently monitored in order to enable a timely reaction to fraud and any risks posed by such activities. Appropriate measures should be in place to limit the impact of fraud.

3.3.3 Appropriate arrangements should be made to ensure that card transactions can be processed even at peak times and on peak days.*

3.3.4 Sufficient evidence should be provided to enable a transparent and easy clarification of disputes between actors.*

3.4 Clearing and settlement*

3.4.1 Clearing and settlement arrangements should ensure an adequate degree of security, operational reliability and availability, taking into account the settlement deadlines specified by the CPS.*

3.5 Business continuity*

3.5.1 3.5.1.* Business impact analyses should clearly identify the components which are crucial to the smooth functioning of the CPS. Effective and comprehensive contingency plans should be in place in the event of a disaster or any incident that jeopardises CPS availability. The adequacy and efficiency of such plans should be tested and reviewed regularly.*

3.6 Outsourcing*

3.6.1 Specific risks resulting from outsourcing should be managed explicitly and appropriately through comprehensive and appropriate contractual provisions. These provisions should cover all relevant issues, for which the actor who outsources activities within the CPS is responsible.*

3.6.2 Outsourcing partners should be appropriately managed and monitored. Actors who outsource activities should be able to provide evidence that their outsourcing partners comply with the standards, for which the actor itself is responsible within the CPS.*

4 The CPS should have effective, accountable and transparent governance arrangements.

4.1 Effective, efficient and transparent processes should be defined and implemented when making decisions about business objectives and policies, including access policies on issuers and acquirers; reviewing performance, usability and convenience of the CPS; and identifying, mitigating and reporting significant risks to its business.

4.2 There should exist an effective internal control framework, including an adequate audit function.

5 The CPS should manage and contain financial risks in relation to the clearing and settlement process.

5.1 The CPS should identify the financial risks involved in the clearing and settlement arrangements and should define appropriate measures to address these risks.

5.2 The CPS should ensure that all selected clearing and settlement providers are of sufficient creditworthiness, operational reliability and security for their purposes.*

5.3 If there are arrangements to complete settlement in the event of an issuer defaulting on its obligations, it must be ensured that any resulting commitment by an actor does not exceed its resources, potentially jeopardising the solvency of that actor. The CPS must also ensure that actors are fully aware of their obligations under any such arrangement, in line with standard 2.*

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.ecb.europa.eu

PDF ISBN 978-92-899-3414-5, doi:10.2866/111557, QB-03-18-172-EN-N