EUROPEAN CENTRAL BANK

EUROSYSTEM

European Framework for Threat Intelligence Based Ethical Redteaming (TIBER-EU)
&
Cyber Resilience Oversight Expectations (CROE)

AMI-Pay

17 April 2018

CROE – why?

- Sets up a more detailed elaboration of the CPMI-IOSCO Cyber Guidance to aid FMIs and overseers in implementing the Guidance and assessing the FMI's compliance against it
- Provides good practices which can be referred to when giving feedback to FMIs regarding assessments in the future
- Takes into consideration the industry best practices, already set out in different frameworks – e.g. *FFIEC Cybersecurity Assessment Tool, the NIST Cybersecurity Framework, ISF Standard of Good Practice, CobiT and ISO/IEC 27001*
- Provides the basis for overseers to work with FMIs over longer term to raise the FMI's maturity level
- Can be used as:
  - Assessment Methodology for overseers; and
  - Tool for self-assessments for FMIs.

Cyber Maturity: The three-level approach

A three-level approach was agreed on due to its advantages:

- In order to adapt to a changing cyber environment, FMIs are expected to continuously evolve on the cyber maturity scale (as also specified in the Guidance);
- Provides an *insight* about the FMI's level of maturity and what it needs to improve in terms of cyber expectations, incentivizing the FMIs to evolve in terms of cyber maturity;
- Takes into account the *proportionality* principle (specific minimum requirements for SIPS, PIRPS, ORPS); and
- Allows the overseers to have a detailed snapshot of the overall sector's level of cyber maturity and what the main challenges for improvement are.

Defining the three levels of an FMI's cyber maturity

Baseline maturity level

- Essential capabilities are established and sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the approved cyber resilience strategy and framework, and
- performance of practices is monitored and managed.

- **All payment systems must meet the Baseline Expectations, aspiring to move to Intermediate level**

Intermediate maturity level

- Baseline maturity level *Plus*
- practices incorporate more advanced implementations that have been improved over time, and
- capabilities are harmonized across the FMI to proactively manage cyber risks to the enterprise.

- **All SIPS must meet the Intermediate Expectations, aspiring to move to Advanced level**

Advanced maturity level

- Baseline maturity level *Plus*
- Intermediate maturity level *Plus*
- capabilities across the FMI are enhanced as needed, in the midst of the rapidly evolving cyber threat landscape, to strengthen the cyber resilience of the FMI and its ecosystem, by proactively collaborating with its external stakeholders.

European Red Team Testing Framework (TIBER-EU)

- **FMIs are required to undertake different forms of testing**, e.g. vulnerability assessment, scenario-based testing, penetration tests, red team tests (CPMI-IOSCO Guidance, chapter 7)
- FMIs are core critical infrastructures, which require tests of the highest standards to be performed: **intelligence-led red team tests**
- Many FMIs are active at pan-European level and/or connected to pan-European settlement platforms (T2 and T2S): **interconnectedness benefits from comparable test standards**
- Red Team Testing Framework for FMIs and FIs is already in place in UK (CBEST) and NL (TIBER-NL), other jurisdictions to follow soon: **risk of fragmentation**.

Need for harmonised approach: European Red Team Testing Framework is currently being developed by Eurosystem

EU Threat Intelligence Based Ethical Red Teaming – TIBER-EU

Key objectives of TIBER-EU

- **Improve the cyber resilience of FMIs** and the sector as a whole, and use testing as a learning experience for improvements;
- **Standardise and harmonise** the way for all FMIs to perform intelligence-led red team tests across the Eurosystem (and possibly the EU), whilst also allowing each authority a degree of flexibility to adapt the framework according to the specificities of their jurisdiction (i.e. TIBER-XX);
- **Facilitate cross-border, cross-regulatory tests** on pan-European FMIs to find the weak spots across jurisdictions;
- Create the protocol for **cross-regulatory collaboration, result sharing and analysis**, and foster mutual recognition of tests across the Eurosystem (and possibly the EU); and
- Be **applicable and useable for any type of institution** (FMIs, banks and insurance companies), although our primary focus would be FMIs.

TIBER-EU is "institution agnostic" and based on frameworks which are already applied to financial institutions

Principles

- **Governance:** Authorities could act in different roles: regulator, overseer, supervisor and/or catalyst. FMIs and FIs volunteer for participation in TIBER-EU based red team testing
- **Assurance:** Mutual recognition between authorities; optional accreditation of testers and testing companies; and attestation by board of FMI or FI
- **Legal & Compliance:** No law to be broken: regulations, data privacy, ethical boundaries apply as normally
- **Collaboration:** To effectively address cyber threats, regulators, market and cyber security industry have to work together
- **Sector Resilience:** Testing framework is meant to contribute to the resilience of the sector as a whole

Process - preparation

1) **Generic threat intelligence report**: what are the relevant cyber threats for FMIs, banks, CSDs and CCPs; who are the cyber threat actors and their Tactics, Techniques & Procedures
2) **Engagement with FMI/FI**: explaining red team process, concept of white/blue/red teams, stakeholder roles and responsibilities, risk management controls, security protocols, contractual considerations and project planning
3) **Scoping**: definition of critical functions of FMI/FI
4) **Procurement**: selecting Threat Intelligence and Red Team Service providers by FMI/FI on basis of minimum standards
5) **Target intelligence**: detailed reconnaissance of FMI/FI based on open source intelligence, development of attack scenarios

Process – actual testing and follow-up

5) **Red Teaming**: deploying attacks on basis of well defined scenarios ("capturing the flags") and in a fully controlled and legally compliant manner
6) **Replay**: red team tester provides report with identified vulnerabilities and recommendations; workshop with red and blue team to review steps taken during test
7) **Remediation Planning**: FMI/FI to draft its remediation plan in close liaison with the respective competent authority
8) **Result Sharing**: competent authorities of pan-European FMIs may share sanitised findings in order to allow mutual recognition and enhance financial sector resilience

TIBER-EU framework expected to be ready Q2 2018, after which it can and will be deployed at national and pan-European level