EUROPEAN CENTRAL BANK

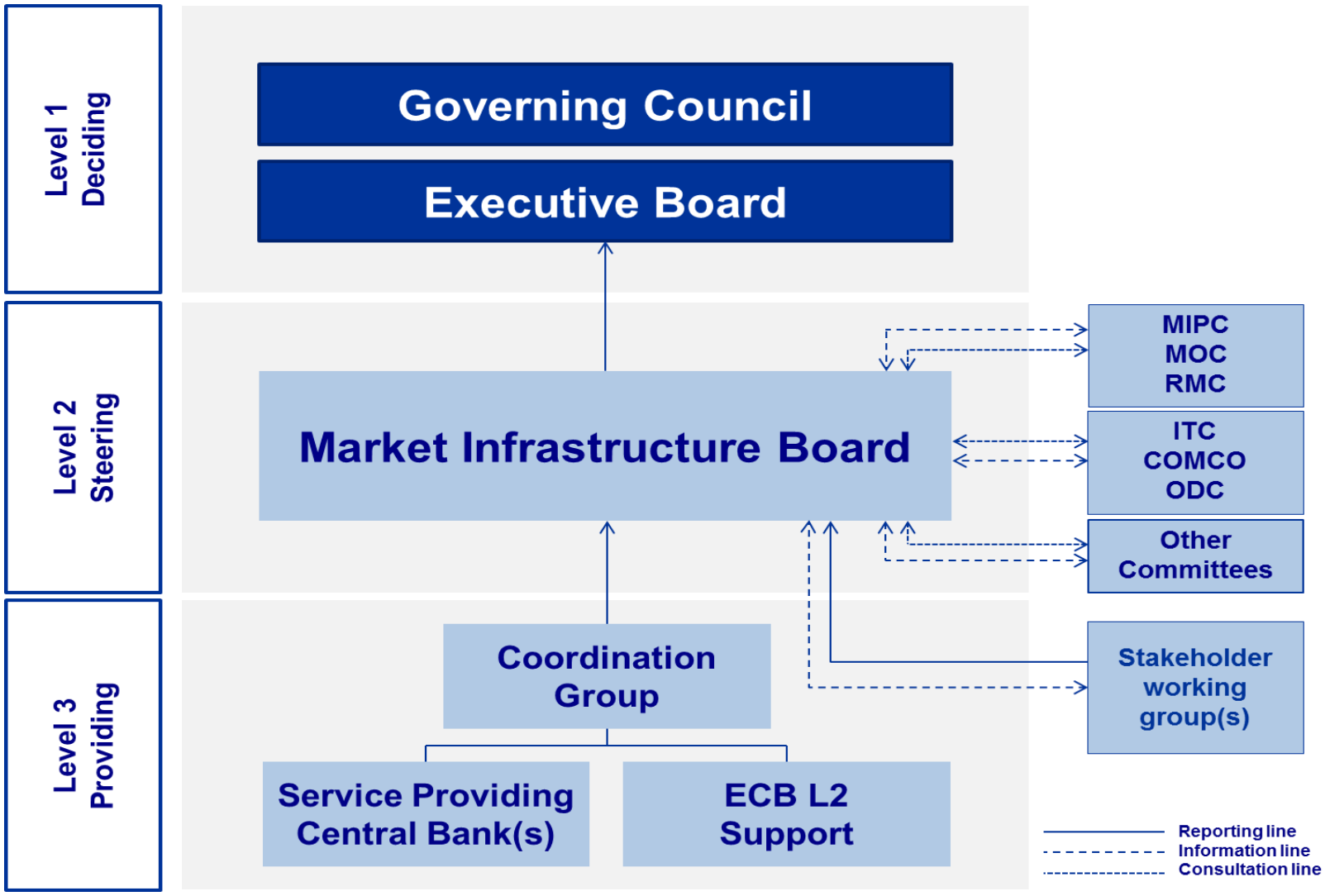
EUROSYSTEM

Francisco Tur Hartmann
European Central Bank

Cyber Resilience for Eurosystem Market Infrastructures

Lima, Peru, 5 February 2019

Eurosystem Market Infrastructures - Governance



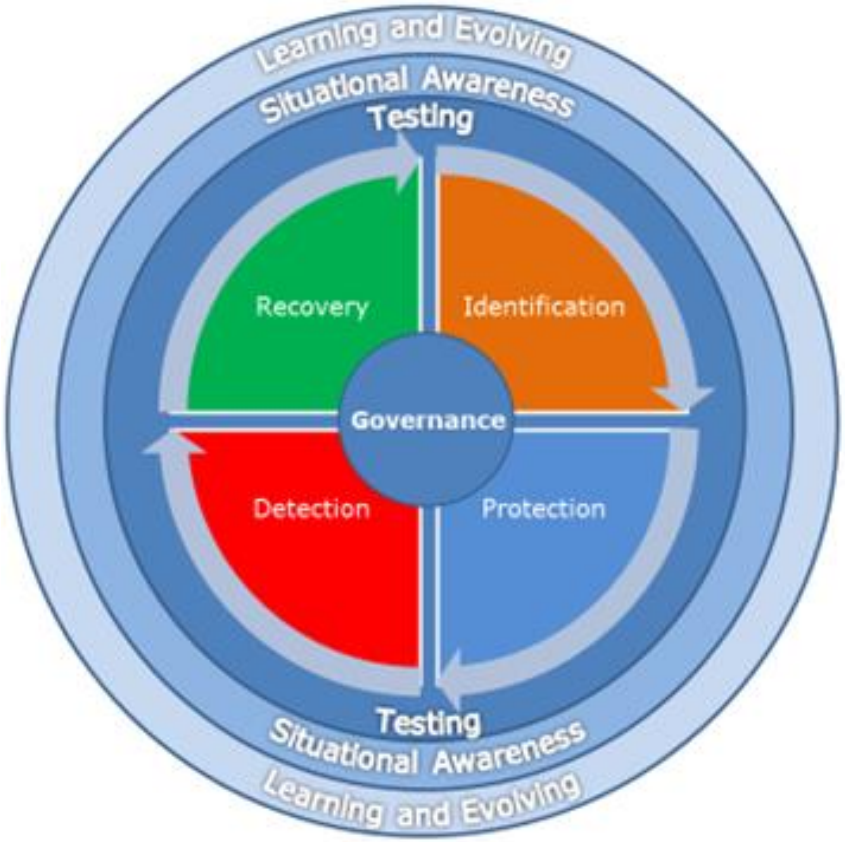
Eurosystem Market Infrastructures - Governance

- The **Market Infrastructure Board (MIB)** is in charge of, among other things, **risk management, cyber resilience and information security issues**, etc. **for the Eurosystem Market Infrastructures** (currently the TARGET Services: the RTGS (TARGET), TIPS and TARGET2-Securities).
- The MIB decided in 2017 on the **Action Plan on Cyber Resilience** (APCR) to enhance the Eurosystem's capabilities regarding detection, prevention, response and recovery against cyber attacks.
- An **enhanced organisational setup** (governance) has also been agreed upon:
  - MIB is responsible for the day-to-day operation of the TARGET Services, as well as the ongoing projects concerning its future enhancements.
  - At the ECB: a dedicated unit (Market Infrastructure Support (MIS) division) supports the operation of the Eurosystem market infrastructures for what concerns financing, risk management, user/acceptance testing, etc.
  - The head of MIS acts as the coordinator of all risks (financial, legal, information security, etc.) and cyber activities for the Eurosystem market infrastructures on behalf of the MIB.

Role of the Market Infrastructure Risk Coordinator (MIRCo)

- The three lines of defence model (as defined by the Institute of Internal Auditors in their 2013 paper on “The Three Lines of Defense in Effective Risk Management and Control”) has been implemented for the Eurosystem Market Infrastructures.
- The 1st line of defence is performed by those involved in the operation (day-to-day management) of the TARGET Services.
- On behalf of the MIB, the MIRCo acts as the 2nd line of defence for the coordination of risks related to the operation of the Eurosystem Market Infrastructures. The MIRCo ensures that:
  - General frameworks for the effective management of risks and complementary frameworks specific for the Eurosystem Market Infrastructures are established and maintained;
  - Complete and effective risk management frameworks are in place for the first and second lines of defence;
  - The risk management frameworks meet the SIPS regulation and other relevant legislation, regulation, standard or guideline;
  - Risks and control are monitored, in support of management and reports to the MIB, provides advice and proposes e.g. enhancements, etc to ensure risks and controls are effectively managed.
- The teams inside the ECB (e.g. financial team, legal team, etc.) and within the Eurosystem (e.g. the Market Infrastructure Cyber Resilience and Information Security (MICRIS) function) support the MIRCo in performing his role.
- The 3rd line of defence consists of the Eurosystem’s Internal Audit Committee (IAC).

CPMI-IOSCO Guidance on Cyber Resilience for FMIs - June 2016



5 risk management categories
3 overarching components

"FMIs should immediately take necessary steps (….) to improve their cyber resilience, taking into account this Guidance."
CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)

"FMIs should also, within 12 months of the publication of this Guidance, have developed concrete plans to improve their capabilities in order to meet the two-hour RTO."
CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)

"Testing is an integral component of any cyber resilience framework."
CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016)

Cyber resilience enhancements

- The following Cyber Resilience **Enhancements** (CREs), prepared in the context of the MIB's Action Plan for Cyber Resilience, have already been approved and are being designed and implemented. These are built on top of (or complement) already-existing capabilities.

  - **Security Services**:
    - Enhancements of the IT infrastructure logging and monitoring with a focus on detection, identification, response and eradication of cyber incidents. Strengthening threat intelligence activities, information sharing, forensic and security awareness capabilities.
    - Enhancements to the collaborative Security Operations Center at the Service Providing central banks

  - **Security Testing**:
    - Thorough security testing of market infrastructures including application testing, penetration testing, red teaming, code reviews and scenario based tests on a routine basis.

Cyber resilience enhancements

- **Data Recovery**:
  - The implementation of technologies and processes to enable the fast and reliable restoration of business data in the event an CR/IS incident occurs.

- **Non-similar facilities (NSF)**
  - The Eurosystem is also analysing enhancements in the context of recovery through non-similar facilities for its TARGET Services to strengthen the contingency capabilities by improving already existing solutions or looking to deploy new ones.

Additional enhancements included in the Action Plan for Cyber Resilience

- **Software Integrity**
  - Further enhancements to increase protection of the Eurosystem Market Infrastructures from tampering of the application and/or system software.
  - To help ensuring the integrity of the system and application software.
  - Detection of anomalies (behaviour-based analytics), raise alerts and ability to restore software from a reliable/trusted source.

- **Enhanced Security Awareness**
  - Security awareness has been developed and maintained through regular re-evaluation and sharing of the lessons learnt within and outside the organisation.
  - The enhanced security awareness service is designed on top of the regular, systematic and continuous training of all employees with access to the FMI's IT infrastructure as well as bespoke training for high risk employees such as administrators or high ranking officials

Additional enhancements included in the Action Plan for Cyber Resilience

- **Information sharing and Cyber Threat Intelligence (CTI)**
  - The collaboration with Eurosystem's Information Technology Committee (ITC) and its substructures is being strengthened via information sharing and cyber threat intelligence initiatives
  - ECB representation (from theT2/T2S operator perspective) in the ITC's dedicated operational security task force.
  - Exchanges on threat landscape on existing and emerging cyber threats against market infrastructures
  - Exploring (further) sources for cyber threat intelligence reports on cyber-attacks targeting the financial sector aiming to the improvement of Sector Resilience

Other work supporting the Cyber Resilience workstream

- **Eurosystem Market Infrastructure Connectivity Guidance (MICG)**
  - After the “Bangladesh case”, in 2016/2017 the Eurosystem developed security requirements for domestic infrastructural components for, initially, TARGET2 participating Central Banks the further increase overall security of the system.
  - This initiative was later on also picked up by SWIFT and SIA/COLT who published the SWIFT Customer Security Programme and the SIA/DOM security guidelines.
  - By end 2018, Central Banks were required to be fully compliant with MICG’s requirements. A new round was also launched in 2019 in order to assess and monitor any potential non-compliance issues in terms of risk exposure until closure.
  - Next evolution steps:
    - extending current MICG to other addressees (e.g. CSDs participating to TARGET2-Securities).
    - Elaborate an interoperability guidance with SWIFT CSP and SIA/COLT DOM in order to limit the burden for the addressees.

Enhancements to the information security frameworks for the Eurosystem infrastructures

- Cyber security landscape
  - Ever-increasing sophistication and proliferation of cyber-attacks.
  - Risk of threats/events potentially affecting confidentiality, integrity or availability of the systems and/or its data is steadily increasing over time.
- Mounting expectations of auditors, regulators and overseers
- Understanding has shifted towards the ***expectation*** **that a cyber-attack/event will eventually be successful** at some point in time
- Enhancing the information security policy for the TARGET Services **geared towards ensuring a continuous evolution and improvement of cyber resilience, information security and recovery capabilities** towards meeting the Eurosystem Cyber Resilience Oversight Expectations (CROE), published in December 2018.

Eurosystem Cyber Resilience Oversight Expectations (CROE)

- 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:
  - As a form of 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 expectations for improving 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.

Three levels of expectations

- **Evolving**: Essential capabilities are established, evolve and are sustained across the FMI to identify, manage and mitigate cyber risks, in alignment with the cyber resilience strategy and framework approved by the Board. Performance of practices is monitored and managed.
- **Advancing**: In addition to meeting the evolving level's requirements, practices at this level involve implementing more advanced tools (e.g. advanced technology and risk management tools) that are integrated across the FMI's business lines and have been improved over time to proactively manage cyber risks posed to the FMI.

  ➔ In the short term, the TARGET Services (T2, TIPS, T2S) will need to aim to attain this level of cyber resilience expectations.
- **Innovating**: Capabilities across the FMI are enhanced as needed within the rapidly evolving cyber threat landscape, in order to strengthen the FMI's cyber resilience and its ecosystem and by proactively collaborating with its external stakeholders. This level involves driving innovation in people, processes and technology for the FMI and the wider ecosystem to manage cyber risks and enhance cyber resilience. This may call for new controls and tools to be developed or new information-sharing groups to be created

EU Threat Intelligence-based Ethical Red Teaming 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 requires 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: a European Red Team Testing Framework to start with

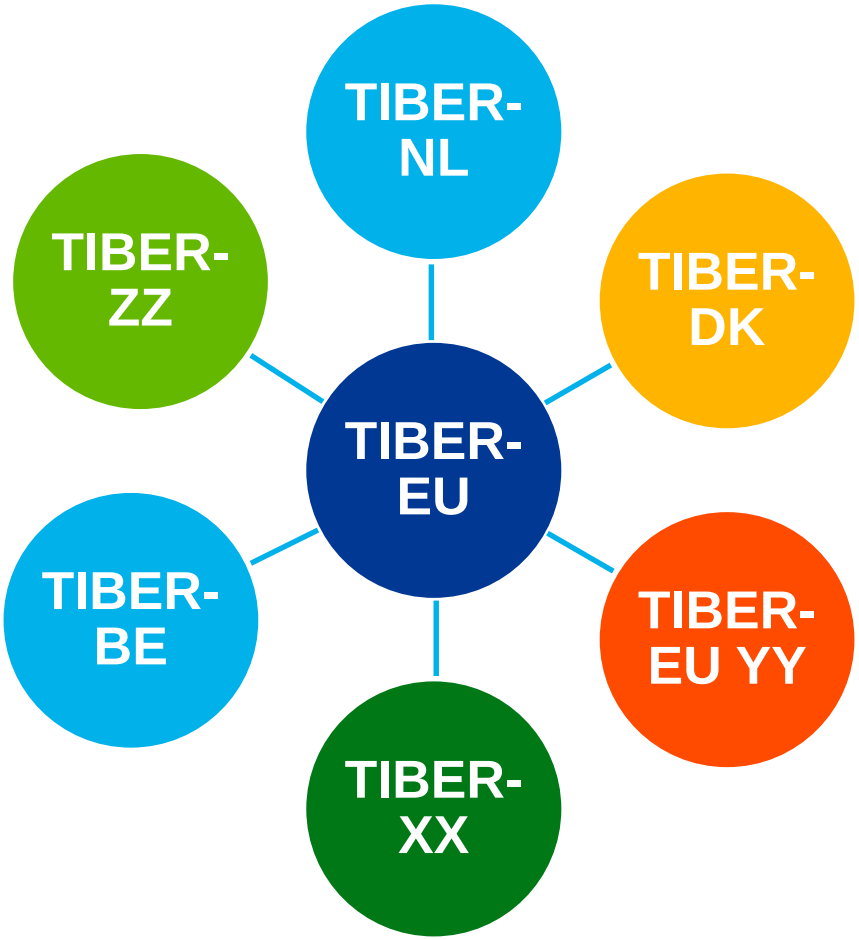
EU Threat Intelligence Based Ethical Red Teaming – TIBER-EU

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 euro-area (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 entity** (FMIs, banks and insurance companies), although our primary focus would be FMIs.

TIBER-EU is “entity agnostic” and based on frameworks which are already applied to financial entities

TIBER-EU vs national TIBER-XX Implementation guides, an example:



Authorities could act in different roles:

1. Regulator
2. Overseer
3. Supervisor, and/or
4. Catalyst

TIBER-EU principles

- **Governance:** Authorities could act in different roles: regulator, overseer, supervisor and/or catalyst. Financial entities 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 financial entity
- **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

Financial entity – and not the involved authorities – bears the first and final responsibility for conducting a TIBER-EU test

TIBER-EU – 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 financial entity**: 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 financial entity
4) **Procurement**: selecting Threat Intelligence and Red Team Service providers by financial entity on basis of minimum standards
5) **Target intelligence**: detailed reconnaissance of financial entity (open source intelligence), development of attack scenarios

TIBER-EU – Process – actual testing & follow-up

6) **Red Teaming**: deploying attacks against critical live production systems on basis of well defined scenarios ("capturing the flags") and in a fully controlled and legally compliant manner

7) **Replay**: red team tester provides report with identified vulnerabilities and recommendations; workshop with red and blue team to review steps taken during test

8) **Remediation Planning**: financial entity to draft its remediation plan in close liaison with the respective competent authority

9) **Result Sharing**: competent authorities of pan-European financial entities may share sanitised findings in order to allow mutual recognition and enhance financial sector resilience

TIBER-EU framework and its Services Procurement Guidelines have been published and are deployed at national and pan-European level

Euro Cyber Resilience Board for FMIs (ECRB) – Key characteristics – industry engagement (dialogue)

Who and what:

- among pan-European FMIs and Critical Service Providers
- between FMIs and the range of different European authorities
- non-technical discussion at Board level about cyber-related topics

Objectives:

- foster trust and collaboration among FMIs and between FMIs and authorities
- catalyse joint initiatives to enhance sector capabilities and capacities, develop solutions and increase cyber awareness

Format objectives:

- avoiding duplication of existing cooperation models
- decisive, but not necessarily formally decision-making

Euro Cyber Resilience Board for pan-European FMIs - ECRB

ECRB – Composition (all board level) – ECB chair

Members

- T2/T2S, EBA Clearing (Euro1, STEP2-T), STET, equensWorldline, Iberpay, RPS, Euroclear Group, Clearstream, LSE Group (Monte Titoli, LCH Clearnet), BME Group (Iberclear), KDPW, EuroCCP, Nasdaq Clearing, Deutsche Börse Group (Eurex Clearing, Clearstream), SWIFT, SIA, Mastercard and Visa

Active participants

- BuBa, BdF, BdE, BdI, DNB, NBB, BCL, ECB *(i.e. Eurosystem lead overseers of above members),* three ESCB NCBs on rotating basis

Observers

- ENISA, ECB/SSM, EBAuthority, ESMA, COM, Europol

Ad hoc invitees

- Other CSPs (e.g. Microsoft, IBM, Amazon), other FMIs, Cyber Security Service Providers, Chair of G7 Cyber Expert Group (BoE)

ECRB – Functioning of the ECRB

Common positions, directions, statements and strategic views

- Common positions, directions, statements and strategic views of the ECRB are adopted by consensus
  Consensus = lack of major disagreement by any members

No formal powers

- The ECRB will have no formal powers to impose binding measures. Members commit on a voluntary basis to the ECRB common positions, directions, statements and strategic views

Working groups

- The ECRB may establish working groups for a limited period of time for dealing with specific work priorities. A group is disbanded as soon as its mandate is fulfilled.

ECRB – Functioning of the ECRB

Transparency and confidentiality

- Outcomes of the work of the ECRB, agendas, documentation and summaries only published when explicitly agreed by all members
- Information and documentation not disclosed by the ECRB are deemed to be of public security

Frequency of meetings

- Twice a year, but at the discretion of the Chair

Secretariat

- The ECB ensures the Secretariat of the ECRB and may be supported by staff of ESCB NCBs.

Resources

- ECRB members are expected to contribute human and financial resources as far as reasonable to the ECRB.