EUROPEAN CENTRAL BANK

EUROSYSTEM

Securing TARGET Services: Protecting Europe's Financial Backbone

Nordic Cyber in Finance Conference

30 October 2024

Francisco Tur Hartmann,
Head of Division, ECB

Agenda

1. Introduction to TARGET Services
2. TARGET Services 3 Lines Model organisation and composition
3. Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures
4. TARGET Services Cyber Resilience Strategy, frameworks, and implementation
5. Cooperation across pan-European financial infrastructures
6. TIBER-EU exercise

1. Introduction to TARGET Services

Developed and operated by the Eurosystem for the free flow of cash, securities, and collateral in Europe

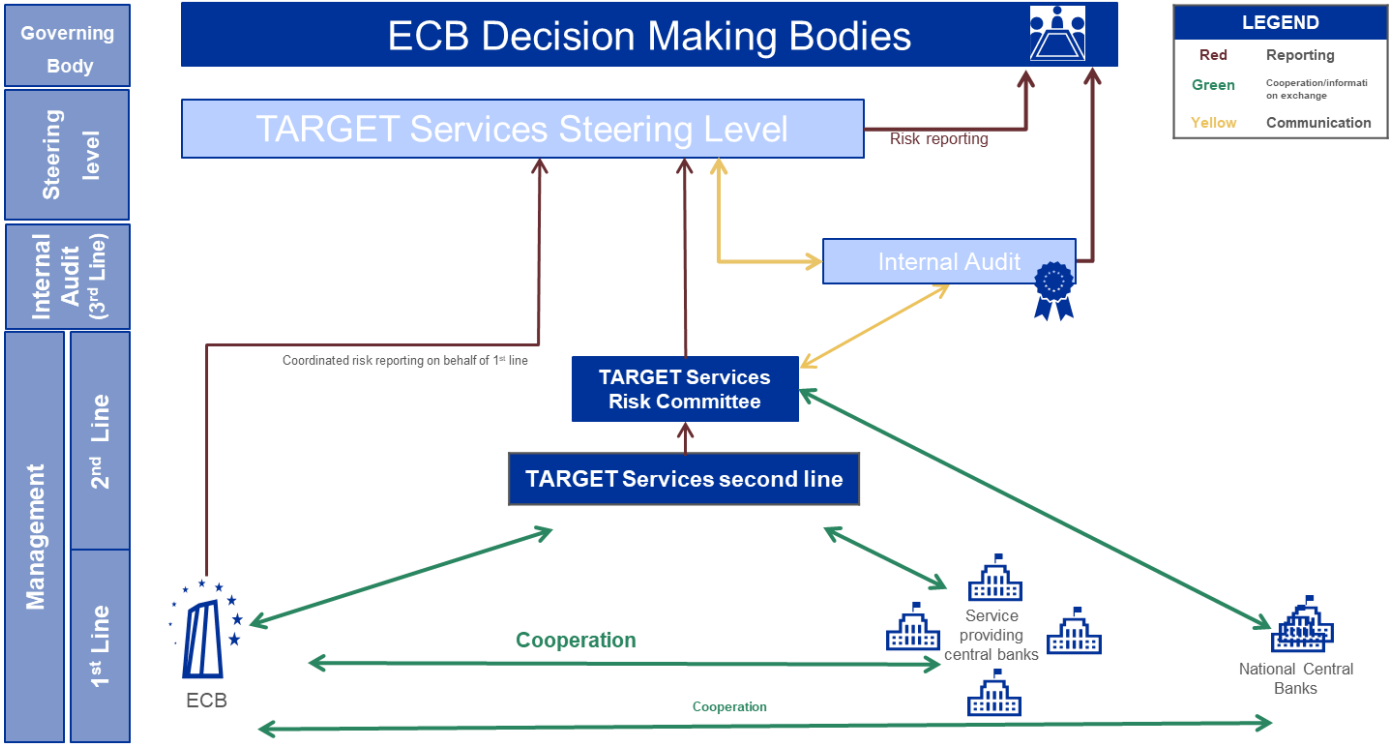
Functions and importance

- Ensures smooth operation of payment systems
- Supports and implements ECB's monetary policy
- Vital for financial stability and economic integration
- Enhances cross-border transactions and market efficiency
- **Protecting** TARGET Services **against cyber threats** is crucial to prevent disruptions and ensure the **reliability of the financial system in the Euro area and beyond**

target services

- **T2: Real-time gross settlement of payments**
- **T2S: Settlement of securities**
- **TIPS: A service for instant payments**
- **ECMS: A service for collateral management [under development]**

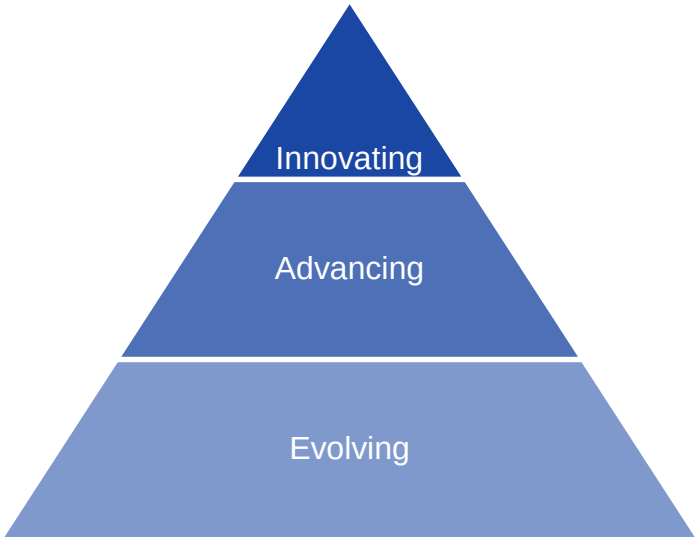
2. Three-lines model to operate and manage the TARGET Services



2.1 TARGET Services 3 Lines Model – composition

	Who	What
1st Line	Operational Management	▪ Ensure **efficient and smooth operations** of TARGET Services on a day-to-day basis. ▪ **Own and manage risks** related to the operation of the TARGET Services.
2nd Line	Risk Management	▪ Defines operational **risk management**, including cyber resilience and information security principles and frameworks for the First Line's implementation. ▪ Reviews the First Line risk assessments and prepares its own **independent risk assessments**, including cyber risks, and proposals for Steering Level submission.
3rd Line	Internal Audit	▪ **Independent review and assurance** of First Line and Second Line activities for risk management.

3. Cyber Resilience Oversight Expectations (CROE) for financial market infrastructures: Maturity levels and Expectations



Evolving

- Basic governance framework
- Initial cyber risk assessment
- Essential protective measures

Advancing

- Enhanced threat detection
- Structured response and recovery plans
- Regular resilience testing

Innovating

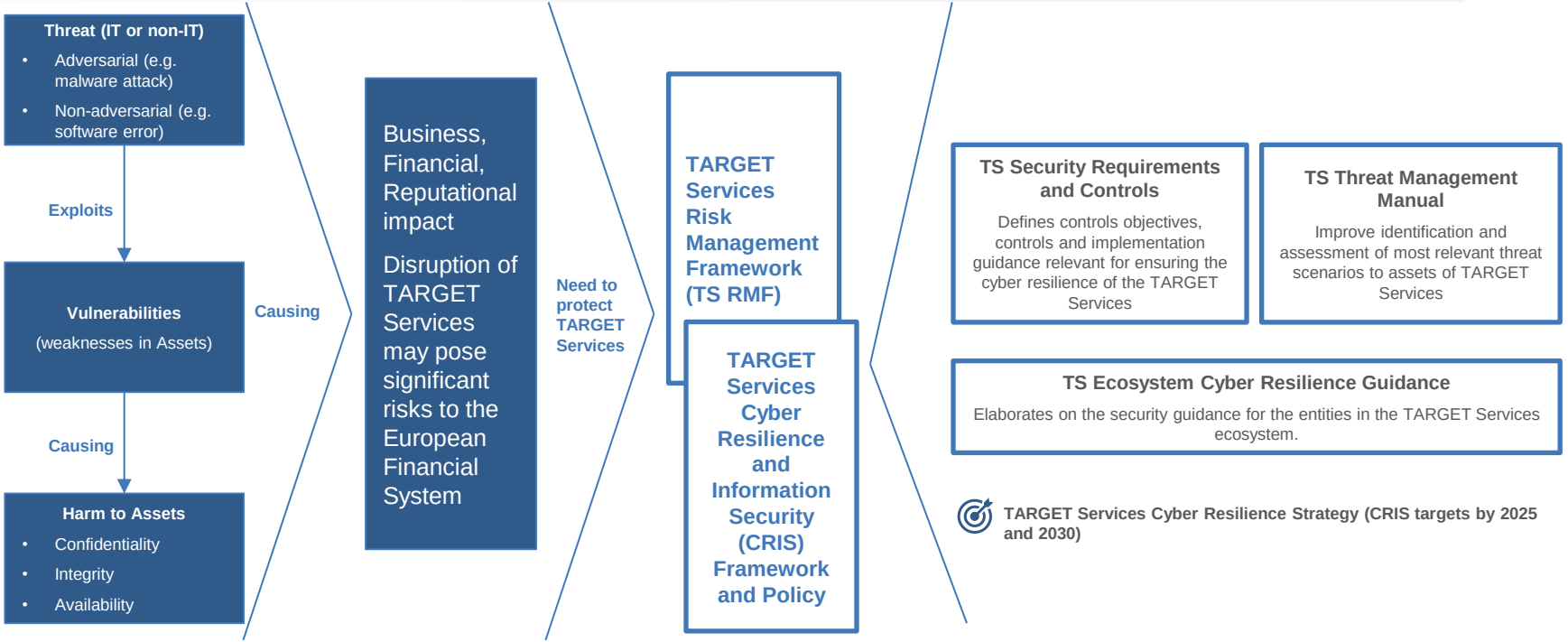
- Proactive threat monitoring
- Utilizing advanced technologies
- Ensuring third-party risk management and resilience

- **CROE is the Framework** developed by the Eurosystem's Oversight function to guide FMIs in enhancing their cyber resilience, helping them to anticipate, withstand, respond to, and recover from cyber incidents.

3.1 TARGET Services follow CROE with the aim to reach innovation level over time

- Financial Market Infrastructures (FMIs) overseen by the Eurosystem must adhere to the revised **Systemically Important Payment Systems (SIPS)** regulation.
  - ➔ Compliance with cyber resilience requirements is assessed using the **Eurosystem Cyber Resilience Oversight Expectations** (CROE).
- This includes T2 and T2S, with T2S mentioned separately as a critical infrastructure rather than a SIPS.
- **T2 and T2S shall**:
  - **reach and maintain the advancing level** of CROE expectations in view of their criticality, and;
  - take active steps to reach the **innovating level** of CROE expectations in the **long term**.

4. TARGET Services Cyber Resilience Framework and Strategy



4.1 TARGET Services Cyber Resilience Strategy implementation

TARGET Services CRIS Framework & Policy

- **Objective:** Ensure TARGET Services stay resilience against evolving cyber threats.

Threat Management

- **Focus:** Evaluate most relevant threat scenarios and their impact on TARGET Services **confidentiality**, **integrity**, and **availability.**
- **Approach:** Use threat scenarios as risk root causes to assess and determine the likelihood and impact of risks to TARGET Services.
- **Integration:** Consider key threat scenarios in recovery procedures and TARGET Services Ecosystem risk management.

T2S External Examination

- **Annual Exercise**: Provides independent assurance for T2S through external examination.
- **Risk Assessment:** Open recommendations are considered in the TARGET Services risk assessment.

5. Cooperation across pan-European financial infrastructures

The Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) Cyber Information and Intelligence Sharing Initiative (CIISI-EU) brings together a community of public and private entities with the aim of sharing intelligence and exchanging best practices.

Types of intelligence shared

- Strategic intelligence: Long-term decision making
- Operational intelligence: Identifying attack patterns
- Tactical intelligence: Understanding adversaries' tools and methods

Impact

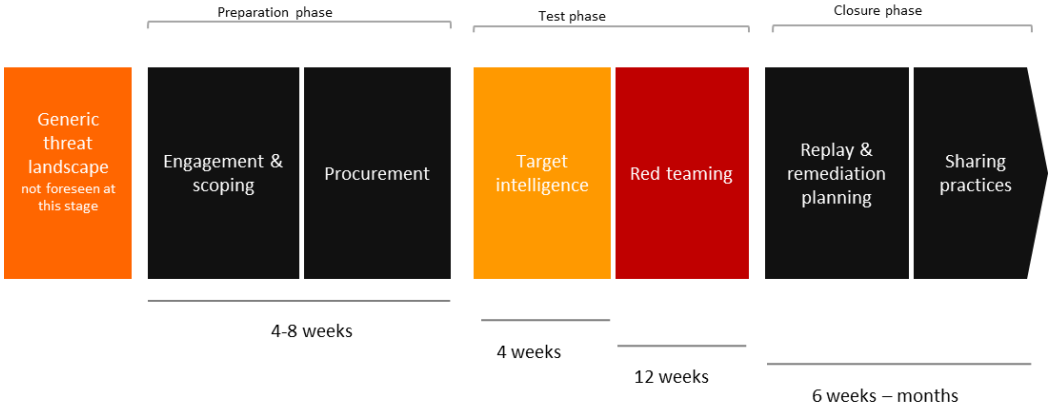
- Enable pan-European financial infrastructures stakeholders to adapt strategies and respond to evolving cyber threats

6. TIBER-EU exercises on the TARGET Services

- The CROE requires to **regularly** perform TIBER-EU tests on the TARGET Services
- Controlled cyber-attack on the **production systems** of the **infrastructure, systems and people** to attempt compromising critical functions of the tested TARGET Service.

  ➔ For TARGET Services, this includes the domestic infrastructure, systems and people of the NCBs providing the TARGET Services

- Provides **additional assurance on the cyber resilience capabilities** of the (Service) Providing national central banks and the tested TARGET Services.



6.1 TIBER-EU exercise on TARGET2 – **highlights**

Objectives

- **Mimic the tactics, techniques and procedures of relevant threat actors** (based on Threat Intelligence)**.** The test needs to respect the **ethical limitations** set by the TIBER-EU framework.
- Managed under a **strict confidentiality** regime.

Outcomes

- Valuable **learning experience** contributing to **further improve the protection, detection and response capabilities**

Leg-ups – to assist the test activity within the test narrative [*due to limited time; restricted capabilities*]

- To test what could have been achieved when an attacker has more time
- To avoid delays during the active test phase (e.g. for establishing an initial foothold or to move laterally closer to the critical systems)
- To ensure reaching the critical functions which are the main scope of the test

6.2 TIBER-EU exercise on TARGET2 – **Actors**

The Referees:

TIBER Cyber Team (TCT)

The TI and RT providers who do the reconnaissance and execute the attack

The people in the entity being attacked and responsible for reacting to the attack. They don't know that it is a TIBER-EU test

The team that know it is a test and are responsible for managing the process and ensure a safe and controlled test. They liaise with the providers and the TCT

6.2 TIBER-EU exercise on TARGET2 – **typical attack steps**

Typical attack path followed by an attacker

- Discovery: **explore** online all types of **information** to gain access to the system(s).
- Initial foothold and persistence: establish an **initial** (stable) **foothold** into the (domestic) **infrastructure** of the targeted entities that operate the targeted critical functions.
- Lateral movement: **move laterally, attempt privileges escalation**, **collect knowledge**, etc. in order to move closer towards the targeted critical systems.
- Execute attack steps: **execute the planned attack** steps.

Two tested scenarios for the exercise on TARGET2

- Threat Scenario 1: Sophisticated state-backed attacker targets the TARGET2 network in a long-term **surveillance and espionage** operation (affecting confidentiality).
- Threat Scenario 2: A ransomware operator attacks TARGET2 in a **double-extortion campaign**(*) (affecting confidentiality, integrity and/or availability)

(*) cybercriminals steal sensitive data and encrypt it. Then, they threaten to release the stolen data unless the victim pays a ransom

Questions?

EUROPEAN CENTRAL BANK

EUROSYSTEM

Thank you for your attention!

FOLLOW US!

@TARGET_ECB

ECB: market infrastructure and payments

https://www.ecb.europa.eu/paym/html/index.en.html