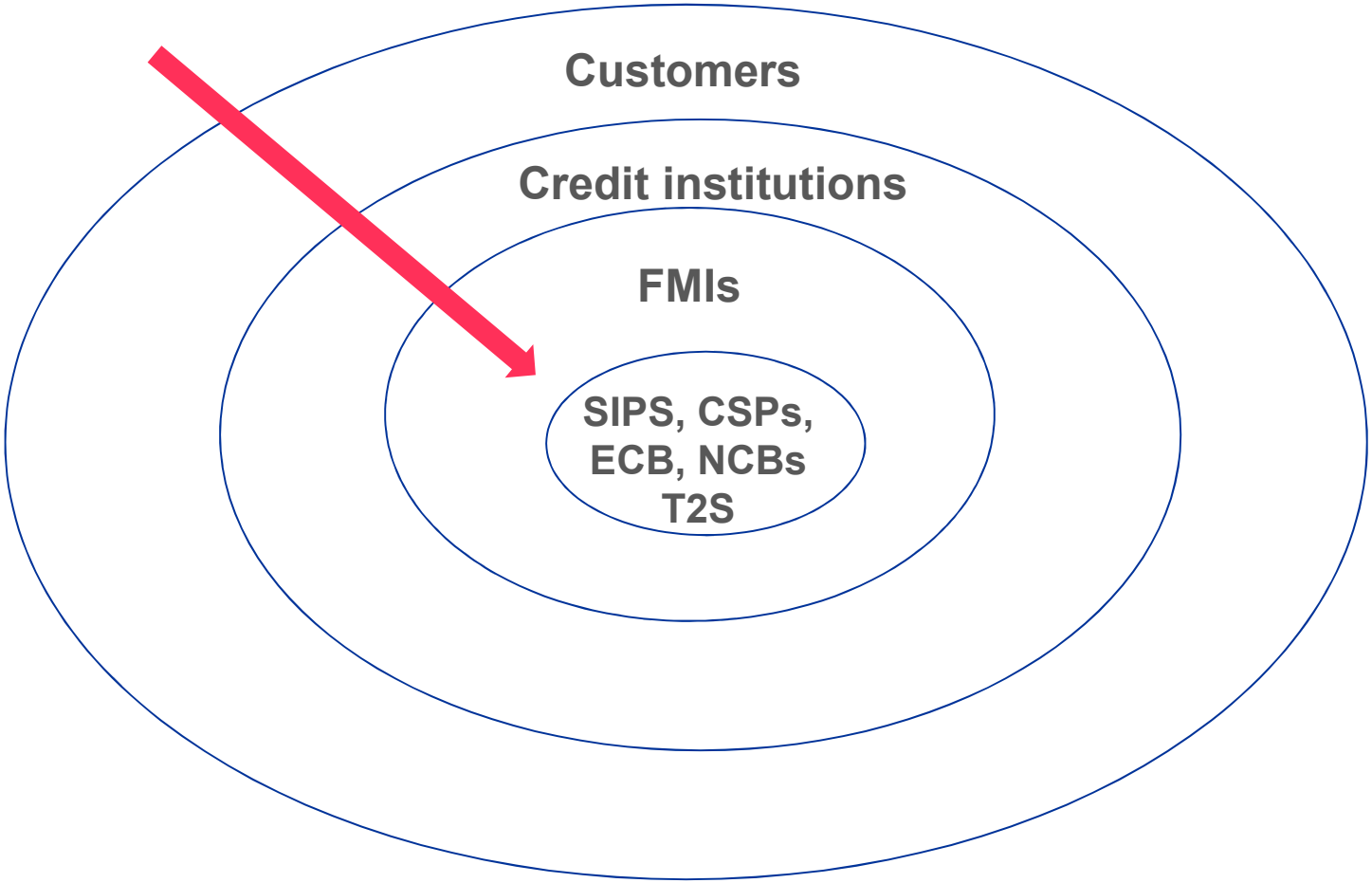
EUROPEAN CENTRAL BANK
EUROSYSTEM

Threat Intelligence Based Ethical Red-teaming (TIBER-EU)

Emran Islam
DG Market Infrastructure & Payments

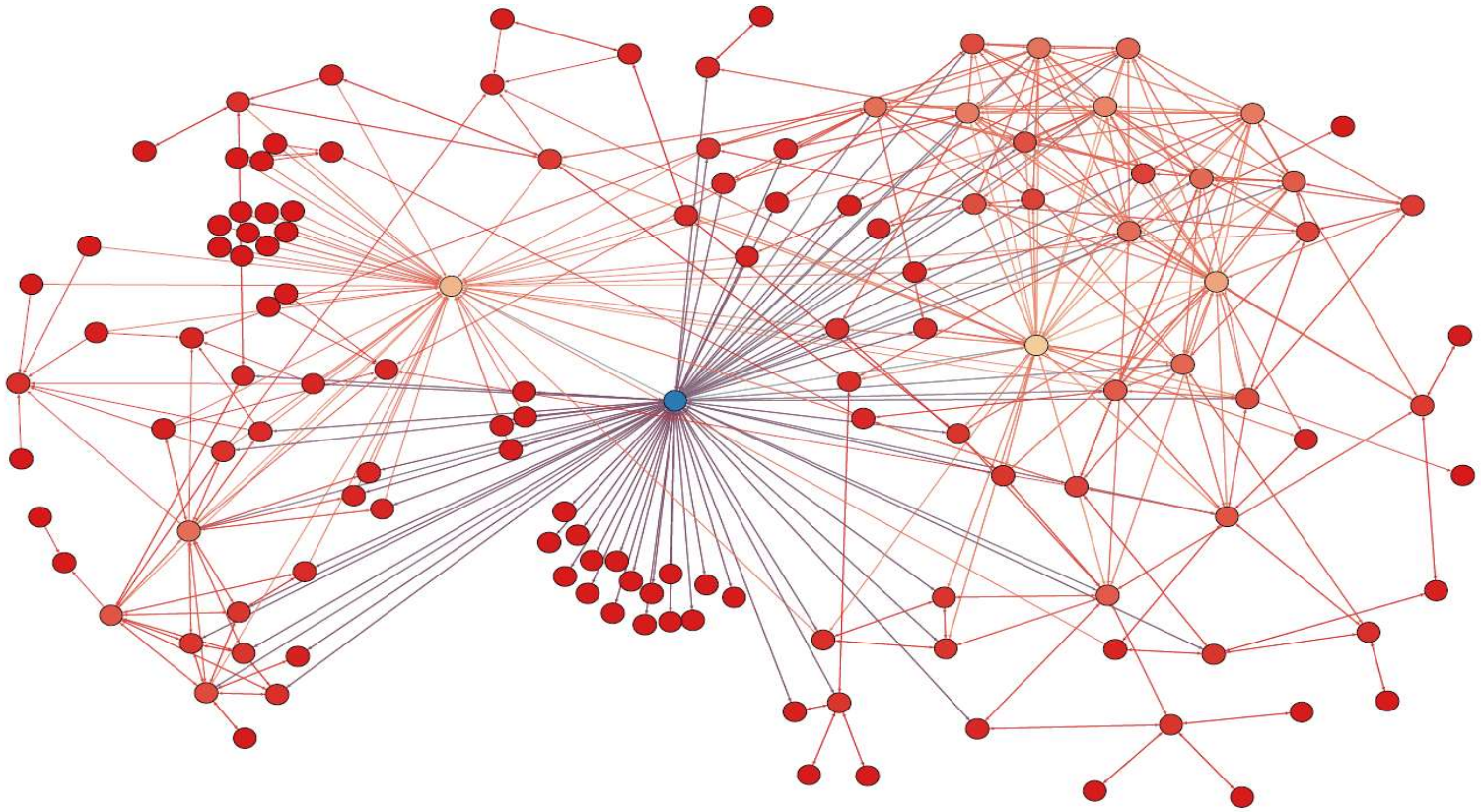
Financial Sector Cyber Resilience Workshop,
CEMLA
Mexico, 7 November 2019

Cyber attackers penetrating the financial system…

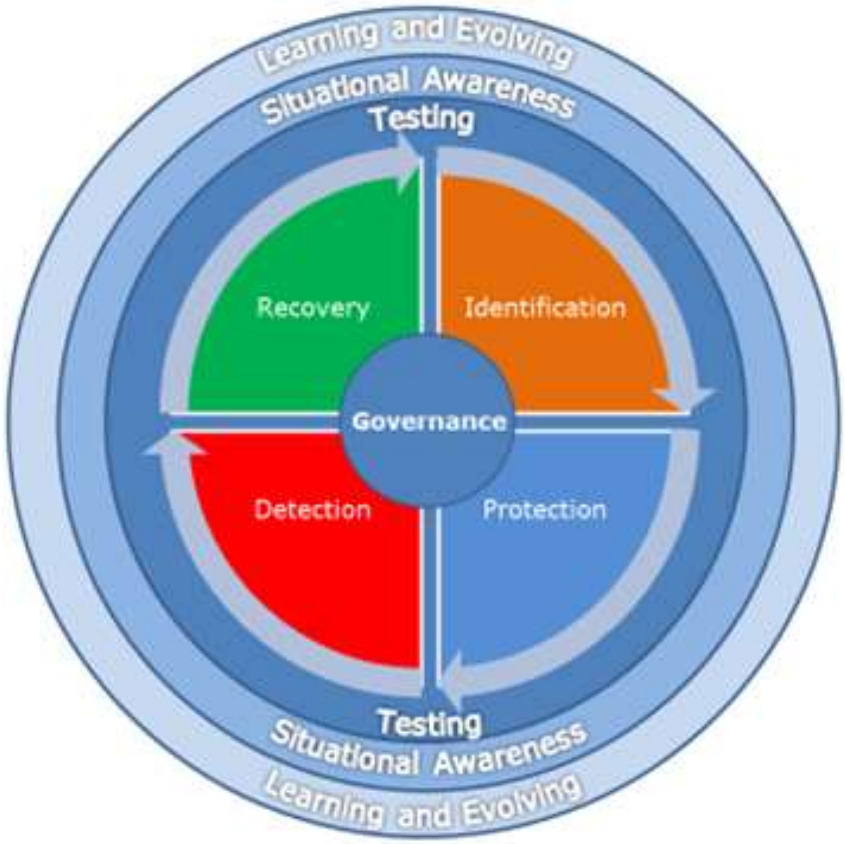


….step by step approaching the core….

Cyber resilience of individual FMIs is key, but it is the resilience of the total financial ecosystem which needs to be ensured



Structure of the CPMI-IOSCO Guidance



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)

Three Pillar Strategy

- ***Pillar 1: FMI Resilience:***
  Cyber Survey, Cyber Resilience Oversight Expectations, TIBER-EU Framework

- ***Pillar 2: Sector Resilience:***
  Market-wide exercising (e.g. UNITAS), information sharing, crisis management, sector mapping, third party risk, ecosystem recovery, cross-authority collaboration

- ***Pillar 3: Strategic Regulator – industry engagement:***
  Establishment of Euro Cyber Resilience Board for pan-European financial infrastructures – market and authorities at Board level

What is Threat Intelligence-based Red Teaming?

Threat Intelligence led Red teaming shows if the threat actor, that is likely to target you, **can**

- **bypass your defensive measures**
- and if so **will they be detected by you?**
- and **what is your response** to this**?**

The goal is to help the entities understand their capabilities regarding protection, detection and response against relevant threat actors and help them improve based on a simulated cyber attack.

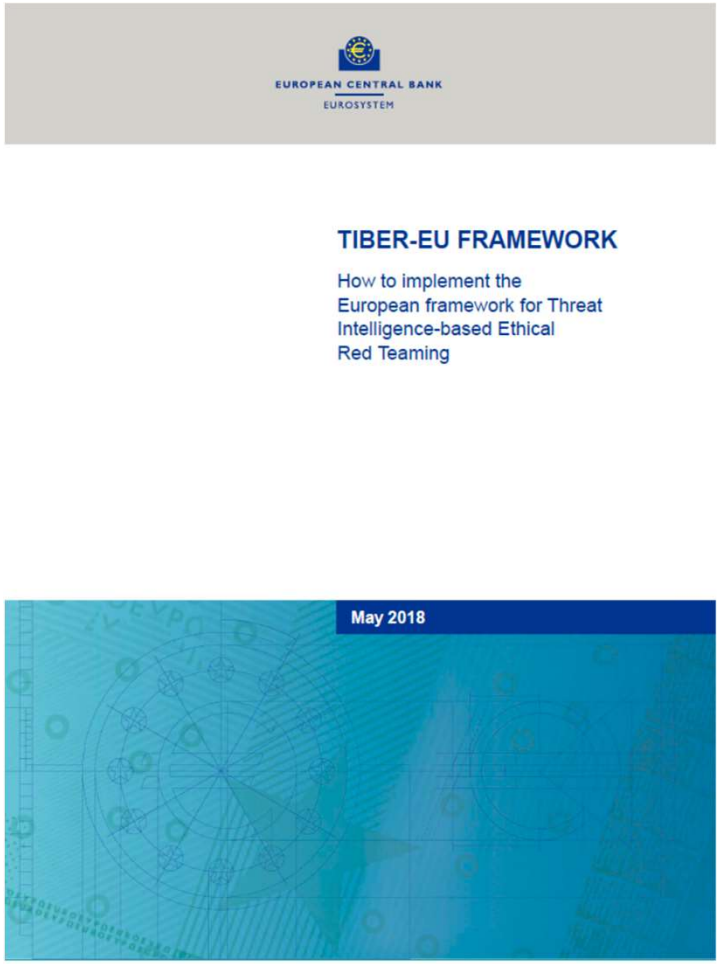
European Red Team Testing Framework (TIBER-EU)

- **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 requires tests of the highest standards to be performed: **intelligence-led red team tests**
- Many FMIs/FIs are active at pan-European level: **interconnectedness requires comparable test standards**
- Red Team (RT) Testing Framework for FMIs and FIs were already in place in UK (CBEST) and NL (TIBER-NL), other jurisdictions were to follow soon: **risk of fragmentation**.

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

EU Threat Intelligence (TI) Based Ethical Red Teaming – TIBER-EU

TIBER-EU framework can also be understood as answer to calls from market participants



Key objectives of TIBER-EU

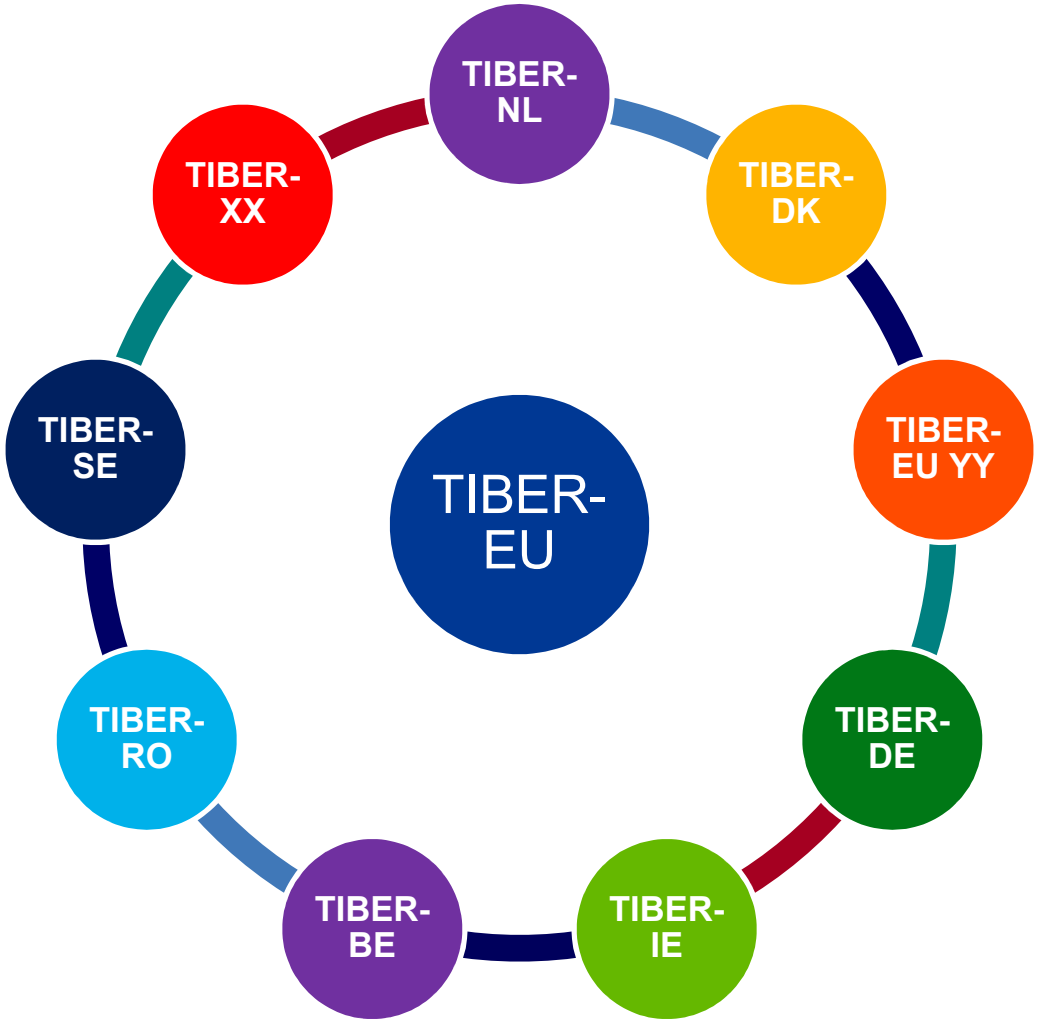
- **Improve the cyber resilience of FMIs** and the sector as a whole, and use testing as a learning experience for improvements;
- **Standardise and harmonise** the way for all FMIs to perform intelligence-led red team tests across the euro-area (and possibly the EU), whilst also allowing each authority 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

Principles of TIBER-EU

- **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

TIBER-EU framework vs. national TIBER-XX implementation guides, an example:



Authorities could act in different roles:

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

The Stakeholders

The Referees:

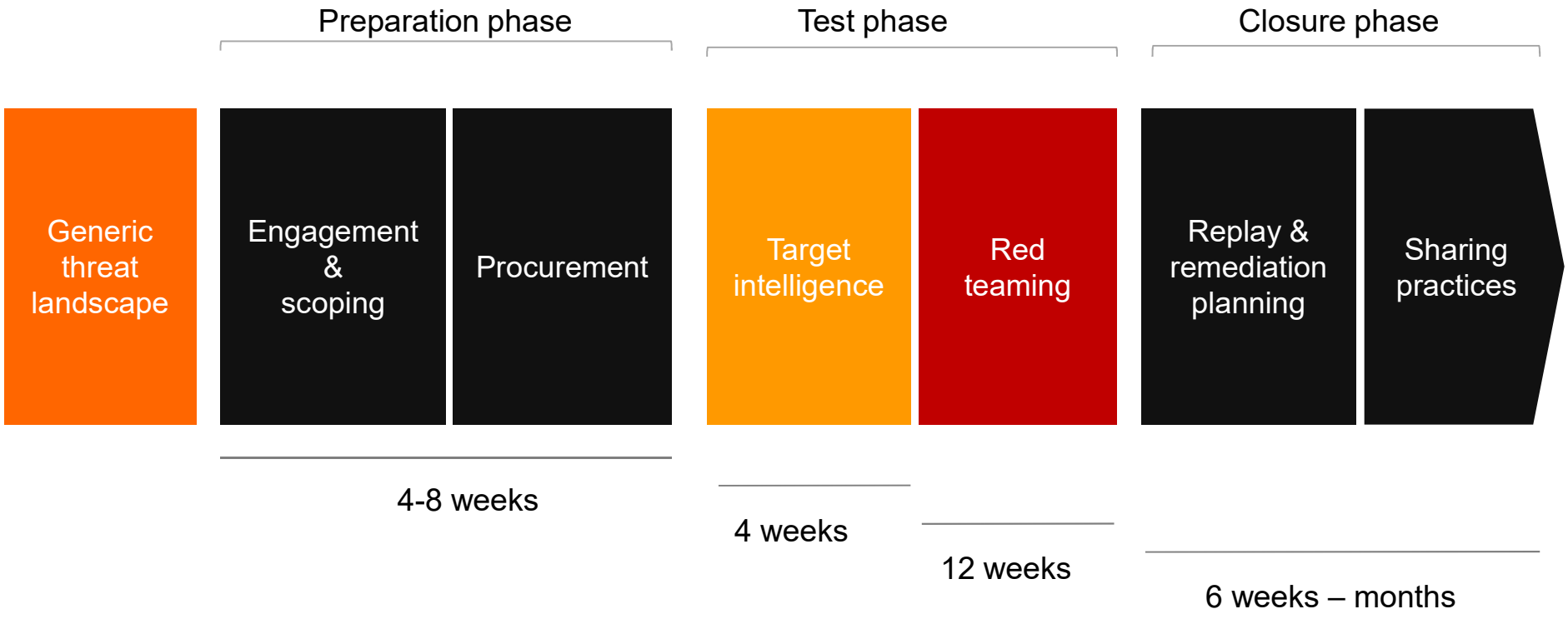
TIBER Cyber Team (TCT)

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

TIBER-EU process



TIBER-EU Services Procurement Guidelines: objectives

- **Risk management:**
  TIBER-EU requires the use of the most **competent, qualified and skilled** Threat Intelligence and Red Team testing providers; requirements are **stringent** to mitigate risks
- **Mutual recognition:**
  Relevant authorities - at national and cross border level - need to have **assurance** that red team tests are performed against mutually agreed upon minimum requirements
- **Market development:**
  Market for TI and RT services is still in its infancy, both at national and at European level. The TIBER-EU Services Procurement Guidelines do serve as **catalyst** for the development of the TI and RT services market

The TIBER-EU Services Procurement Guidelines are an integral part of the TIBER-EU Framework

Requirements of the TIBER-EU Services Procurement Guidelines

Requirements are set at three levels:

- **TI and RT provider level**:
  the TI and RT **company**
- **Managerial level**:
  the TI or RT **manager** responsible for the end-to-end management (of the threat intelligence for) the test

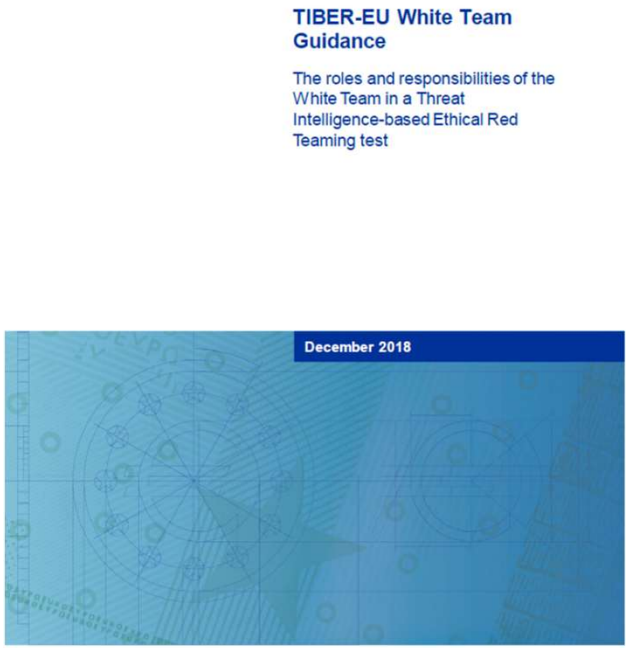
- **TI or RT team level**: **team - and its members** (except its manager) - responsible for delivering the threat intelligence or conducting the red team test.

Requirements refer to references from previous assignments, minimum years of experience, team composition, background checks, etc.

TIBER-EU White Team Guidance

- Guidance for the team leading the test from the entity being tested. They are the only people within the entity that know that a test is undertaken.

- Different functions:
  - White Team Lead
  - Subject matter Experts
  - C-level involvement
  - Other needed expertise ad hoc
    - Legal, procurement etc.



Next steps

- Respective **competent authorities** to **adopt** the framework, to **apply** it to their formal remit, and to **adapt** it - using the optional features – if needed to the specificities of their jurisdiction (i.e. TIBER-XX);
- **Financial entities (e.g. Financial Market Infrastructures and banks)** are encouraged to liaise with their relevant authorities and cooperate to establish a framework that will enhance the cyber resilience of their sector.
- **Threat Intelligence and Red Team providers** are encouraged to consider their resources and capabilities to ensure that they meet the required standards in delivering bespoke, intelligence-led red team tests for entities

- Cyber resilience of financial ecosystem is a **joint effort** of institutions, infrastructures and regulators
- Threat Intelligence Based Ethical Redteaming is **essential tool** to test cyber resilience of critical FMIs/FIs (but not the only one…)
- The TIBER-EU framework ensures **pan-European harmonisation & cooperation**, is **entity agnostic**, and **avoids pan-European FMIs to undergo multiple tests**
- Each authority has a degree of flexibility to adapt the framework according to the specificities of their jurisdiction (i.e. TIBER-XX);
- Authorities could act in different roles: regulator, overseer, supervisor and/or catalyst;
- Performing the test is the **responsibility of the to be tested entity**

Questions

Useful links

CPMI-IOSCO "Guidance on cyber resilience for financial market infrastructures"
www.bis.org/press/p160629.htm
www.bis.org/cpmi/publ/d146.pdf

TIBER-EU Framework, Services Procurement Guidelines and White Team Guidance
www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html
www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf
https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf

Mandate ECRB
www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1.en.html
www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180309_1/ecb.sp180309_1_ECRB_mandate.pdf

UNITAS crisis communication exercise
https://www.ecb.europa.eu/pub/pdf/other/ecb.unitasreport201812.en.pdf

CPMI Report "Reducing the risk of wholesale payments fraud related to endpoint security"
www.bis.org/press/p180508.htm
www.bis.org/cpmi/publ/d178.pdf

G7 Fundamental Elements of Cyber security in the Financial Sector
https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en

ECB Cyber Resilience Oversight Expectations (CROE)
https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr181203_1.en.html
https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

FSB Cyber Lexicon
http://www.fsb.org/2018/11/fsb-publishes-cyber-lexicon/
http://www.fsb.org/wp-content/uploads/P121118-1.pdf