CPMI Cyber guidance

Operationalization at DNB

Evert Fekkes, November 2019

DeNederlandscheBank

EUROSYSTEEM

Five key messages from the guidance

1. **Board and governance is critical**
2. **Understand the battlefield**
3. **Learn and evolve**
4. **Safe and quick resumption**
5. **Collective resilience**

Two examples implemented in Europe:

- TIBER – Threat Intelligence Based Ethical Red Teaming
- CROE – Cyber Resilience Oversight Expectations for FMIs

Varying shades of red

Financial Stability Institute – FSI Insights No 21, November 2019

- In general, a red team test can be divided in four phases: reconnaissance; getting into the institution; getting through its systems; and getting out with the captured “flags”
- An effective test is characterised by both firms and authorities being open about the results, learning from the weaknesses exposed and taking appropriate remedial actions
- Sound technical and business expertise on the part of those involved in red team tests within firms, external threat intelligence and test providers as well as authorities is particularly important to ensure high-quality tests

Learn and evolve: cyber resilience testing

Threat **I**ntelligent **B**ased **E**thical **R**ed **T**eaming

- Internal team and program within DNB
- Guiding role creates authority
- Warrant the required level of testing through applied guidelines

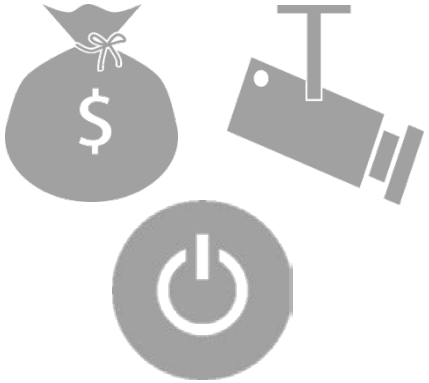
Cooperation on the highest level (Financial Stability Committee)

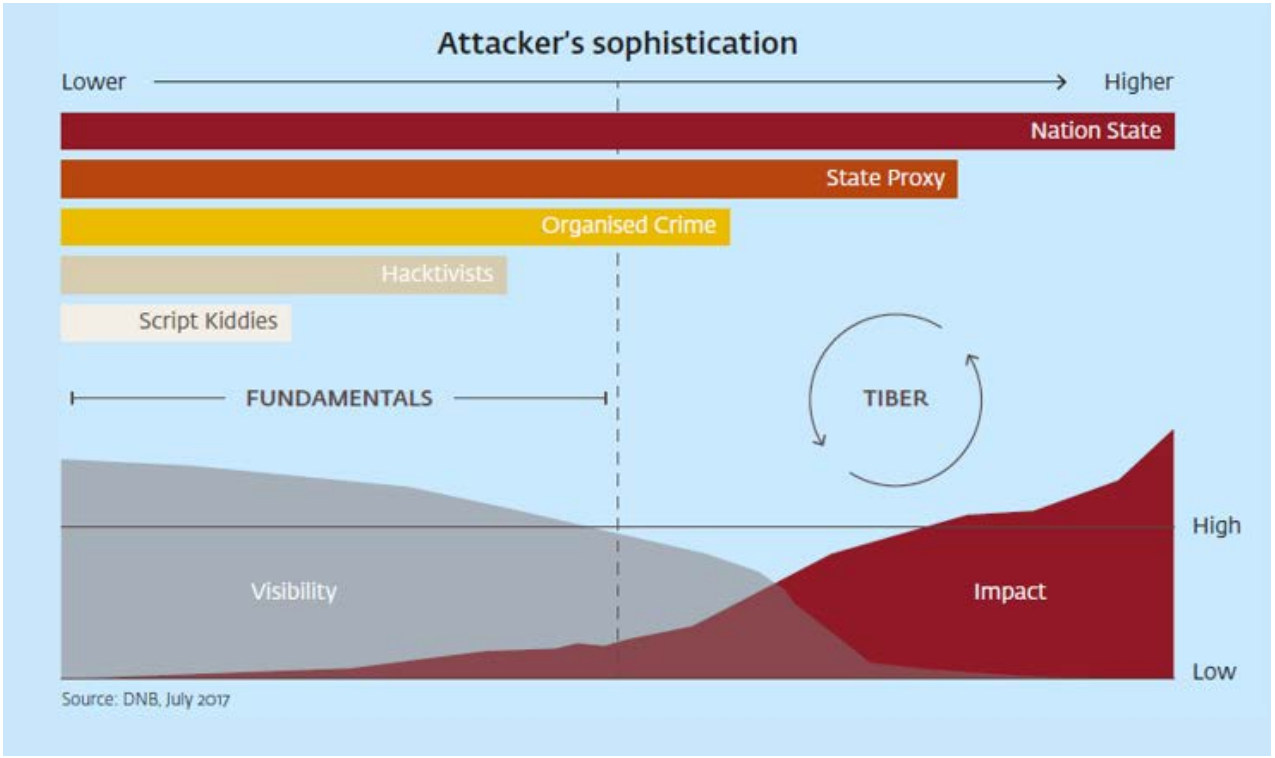
https://youtu.be/-dXf96mot2A

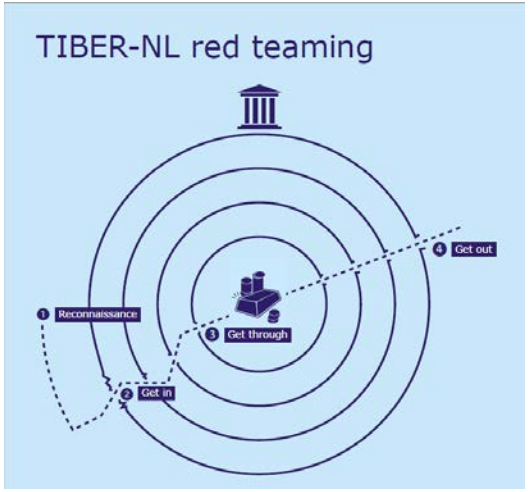
Characteristics of red team testing

Characteristic	Red team testing	Penetration testing
Objective	To test resilience against realistic attacks in order to identify potential weaknesses in an institution's protection, detection and response capabilities	Gain insight into system vulnerabilities
Scope	Objective-based, open-scoped, designed to demonstrate critical impact to a business or organisation. Targets people, process and technology	Limited-scope technical assessment
Attack surface	Everything is "on"; scoped by white team*	Scoped by blue team
Defensive informed	Defensive team not informed beforehand	Defensive team informed and included in scoping of activities
Post-exploitation	Extensive focus on critical assets and functions	Very limited
Tested controls	Focus on protection, detection and response	Focus on protection
Test methods	Focus on realistic simulation; testing includes technical, human and physical factors	Focus on efficiency; testing includes mostly technical factors
Test techniques	Tactics, techniques and procedures (TTP)	Mapping, scanning and exploiting
Testing live systems	Live production systems	Typically limited interaction with live production systems
Duration	Months	Weeks

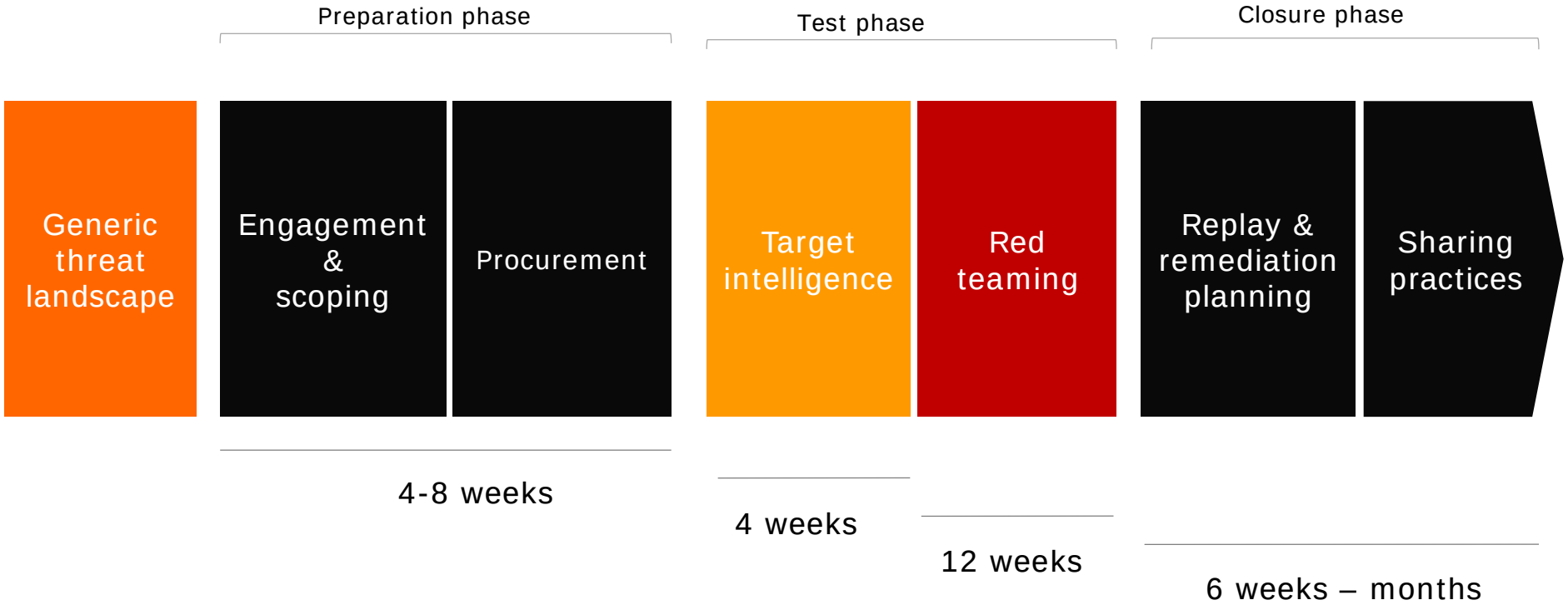
Understand sophistication of attacks



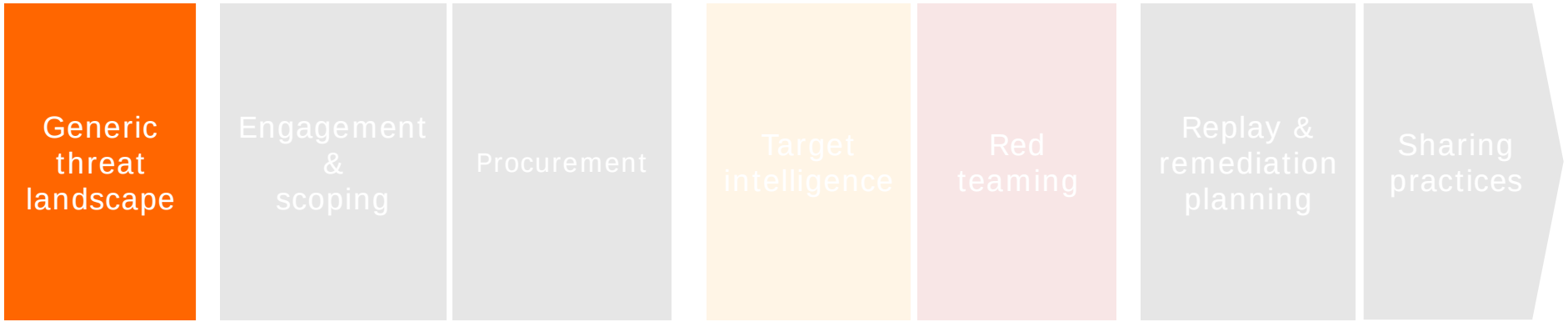




TIBER: understand, assess, evolve



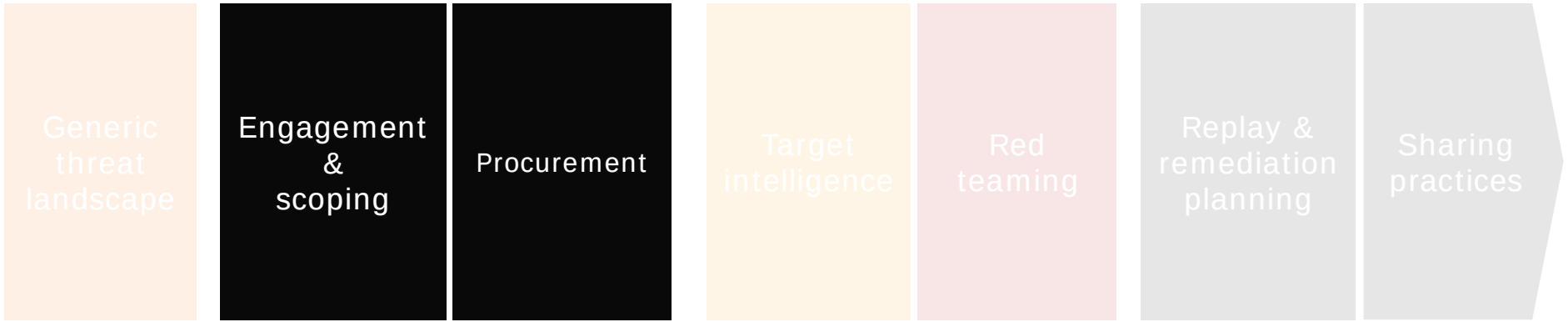
TIBER-NL



Generic threat intelligence

NL financial critical infrastructure, divided in: Retail banking, Wholesale, Clearing and settlement, Stock exchange

TIBER-NL

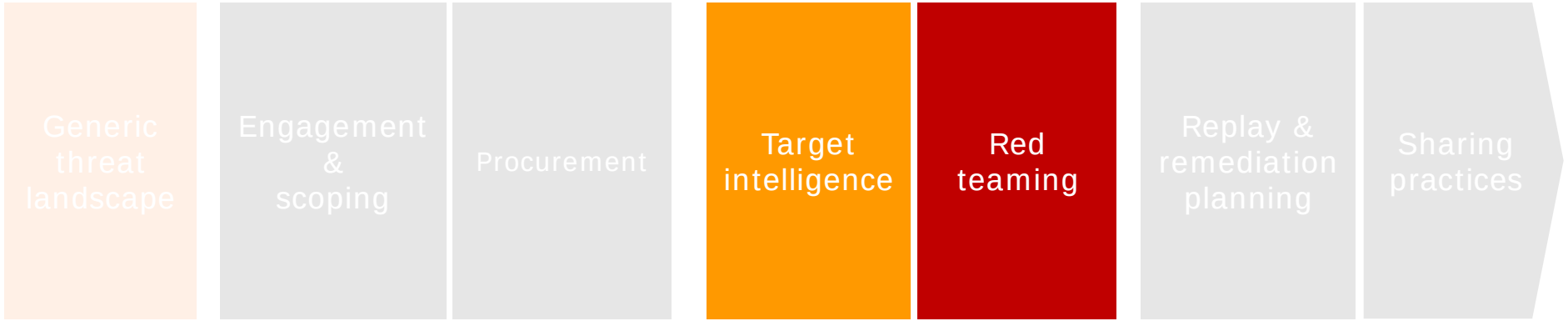


Critical economic functions, selected key systems and services

Potential compromise actions

Highest standards TI and RT (procurement)

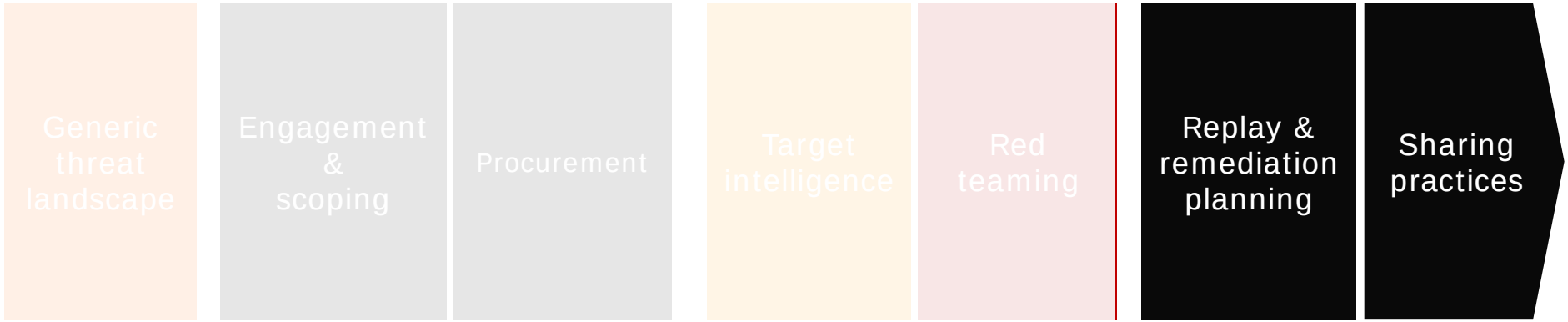
TIBER-NL



Institution's attack surface: People, process and technology
- In
- Through/Out

+ Scenario X

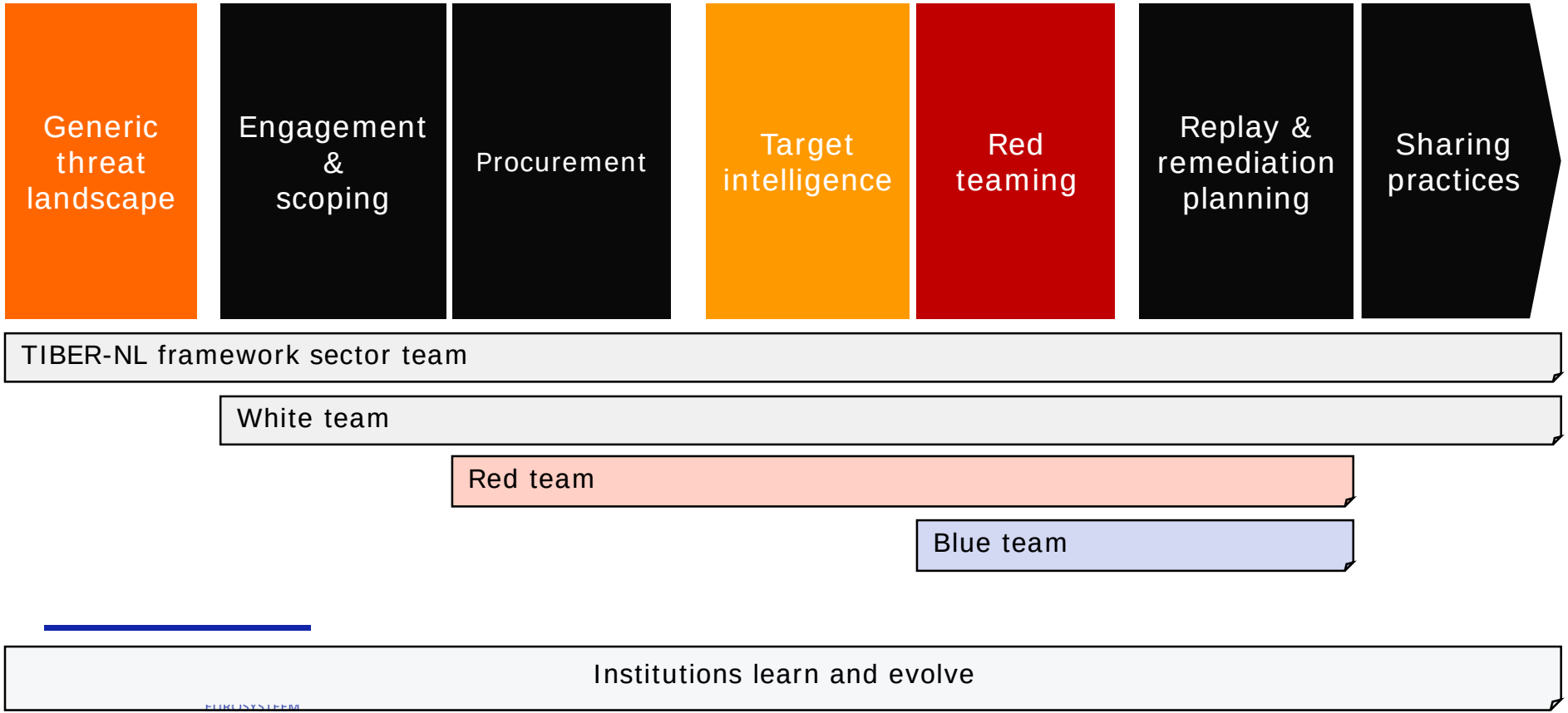
TIBER-NL



Replay (red and blue team, purple teaming)
Remediation

Learning experience by institution self
Sharing good practices with TIBER-NL participants

TIBER-NL:framework roles and involvement



TIBER-NL: participants 2019-2022

Financial core infrastructure

Pension funds

Insurance companies

DeNederlandscheBank
EUROSYSTEEM

Oversight on payment security

- Principle based approach
  - NIST basis for guidance on cyber resilience

    Identify, Protect, Detect, Respond
  - CPMI guidance: application for FMIs
  - Eurosystem Cyber Resilience Oversight Expectations for financial market infrastructures (CROE)
  - Swift CSP, PCI-DSS, ISO 27001, …

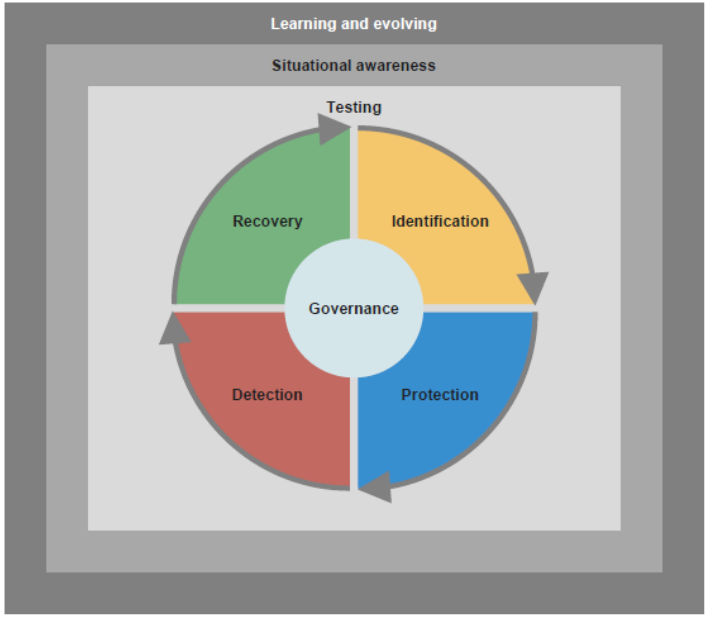
ECB CROE – a benchmark for overseers

The cyber resilience oversight expectations (CROE) serves the following three key purposes:

(i) it provides FMIs with **detailed steps** on how to operationalise the Guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time;

(ii) it provides overseers with **clear expectations** to assess the FMIs for which they are responsible; and

(iii) it provides the **basis for a meaningful discussion** between the FMIs and their respective overseers.



Risk management categories

CROE – not to be considered a checklist

- The CROE should **not, however, be considered a checklist** of measures with which FMIs must strictly comply. They should instead be **considered a set of practices** that can help FMIs to comply with the Guidance. It will be for the overseers or supervisors to judge whether the FMI, commensurate with its criticality, is meeting the evolving, advancing or innovating levels.

- The overseer's or the supervisor's **professional judgement** is an essential factor in determining whether the FMI is meeting the levels of expectation. This judgement should be driven by a number of considerations, such as: the local laws and regulations governing the FMI; the overseer's or supervisor's broader historic knowledge of the FMI; the FMI's size, criticality and business model, which should ensure a proportionate approach is taken; and the ongoing discussions between the overseer or supervisor and the FMI.

Emerging practice

- We have enough standards now, focus on implementation.

  The ECB CROE is a supporting tool, “points to consider”

- Annual Target2 self assessment for RTGS

- Evaluations: were the resilience processes effective?

  E.g. patch management; firewall rules

Emerging practice

- We should not assume that hackers can be kept outside.
  So behind the front door all controls should be in place.
  It is not (only) about perimeter security.

- TIBER testing shows weaknesses even when the assessment had a “green” result, creating awareness at board level

1. **Board and governance is critical**
   - The CROE sets the expectations regarding governance, board responsibility, risk management, etc.
   - Tiber is the proof of the pudding and shows the resilience is strong enough.
2. **Understand the battlefield**
   - The CROE sets the expectations regarding threats and vulnerabilities
   - Tiber shows whether these are identified thoroughly enough
   - DDoS risks increase; measures should be kept up-to-date and cooperation is necessary
3. **Learn and evolve**
   - Assessments against the CROE and Tiber test evaluations are very helpful regarding improvement of procedures, technical measures and dependencies on people.
4. **Safe and quick resumption**
   - The CROE specifies the expectations.
   - Tiber helps also testing crisis management in practice.
5. **Collective resilience**
   - Cooperation with all the stakeholders in the payment chain is necessary.