EUROPEAN CENTRAL BANK

EUROSYSTEM

Threat Lead Penetration Testing: TIBER-EU framework

concept and implementation

Wiebe Ruttenberg
Senior Adviser
DG Market Infrastructure & Payments

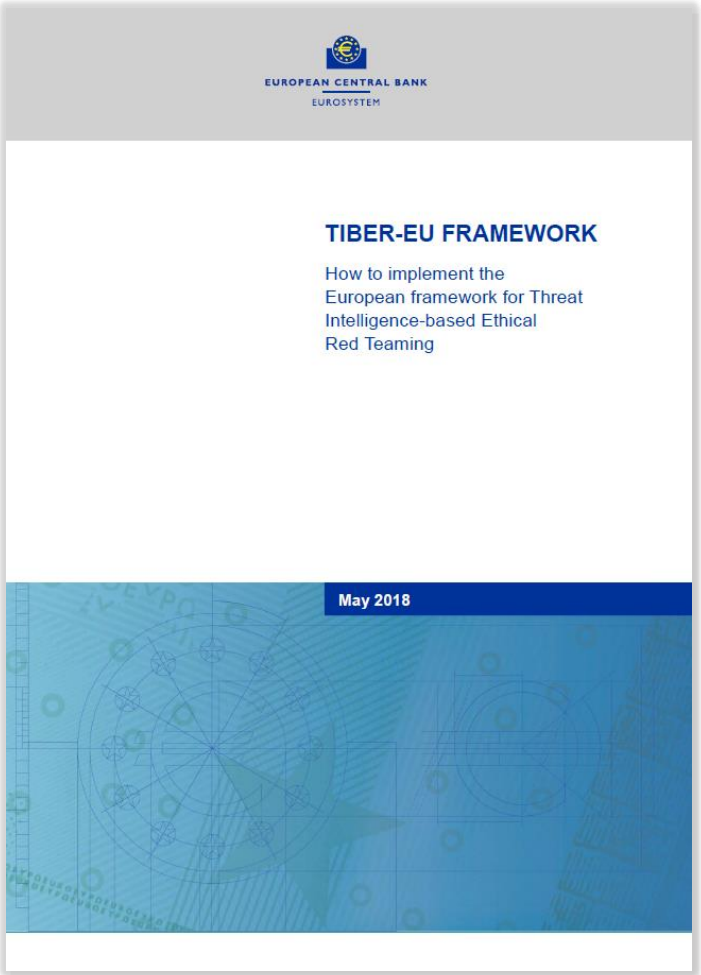
ASBA - CEMLA - FSI event on Cyber Resilience Testing (online, 3 Nov 2020)

If the proof of the pudding is in the eating……..,

… then the proof of cyber resilience is in the testing!

Your own testing cookbook for free:

TIBER-EU framework (May 2018)



TIBER-EU: EU Threat Intelligence Based Ethical Redteaming

EU framework for ethical hacking

- Definition of ethical hacking/ red-teaming
- Recommendations how to do it
- Guidelines how to hire ethical hackers
- Different roles & cooperation models for authorities

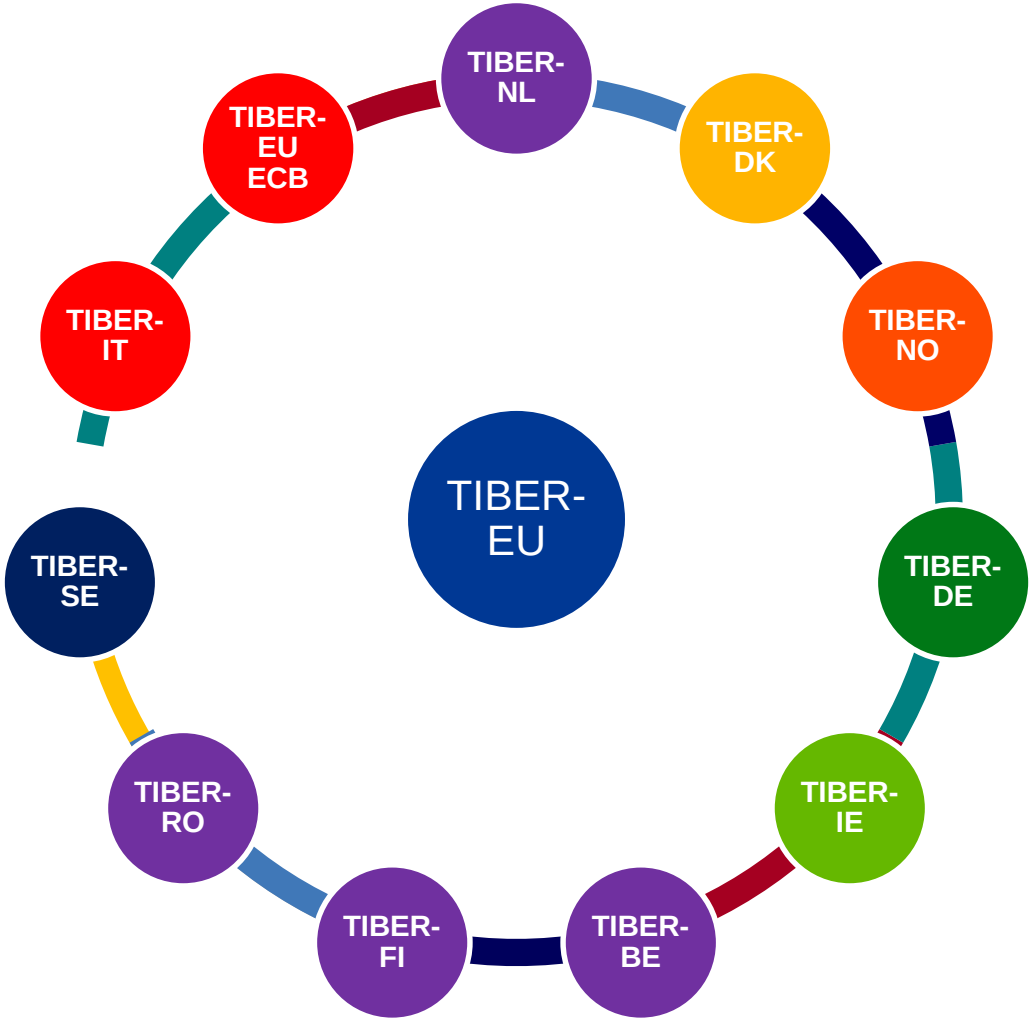
TIBER-EU is “entity agnostic” and based on frameworks which were already applied to financial entities

TIBER-EU key elements

- Goal is to strengthen the cyber resilience of the entities against advanced cyber attackers aiming financial stability
- At the heart lies: collaboration, evidence, learning & improvement
- **No pass or fail test**
- Executed on live production systems
- Intelligence led in order to emulate advanced attackers
- Test followed by independent TIBER-EU test manager(s) from the authority
- Test performed by external, independent third-party providers (Threat Intelligence & Red Team providers)

The responsibility for the test is with the respective financial institutions and financial market infrastructures

TIBER-EU framework vs. national TIBER-XX implementation guides, current status:

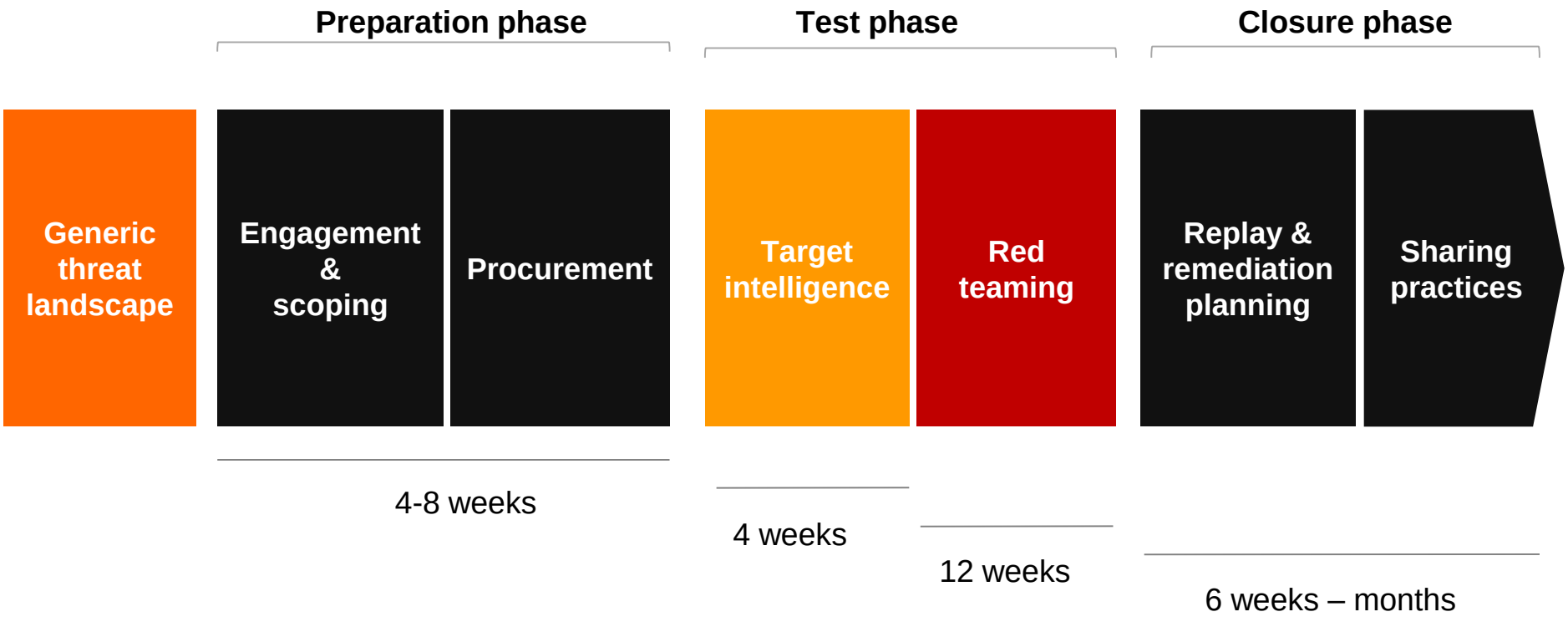


Authorities could act in different roles:

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

Next to that, authorities could agree to be **lead**, or to be **relevant** authority

TIBER-EU process from start to finish



Whole process can easily take up to one year (or more…)

Questions