NIS Directive User Community

NIS, DORA and TIBER-LU: focus on the financial sector

11 May 2022

Cécile Gellenoncourt & Jean de Chillou

Supervision of information systems

cssf

Commission de Surveillance
du Secteur Financier

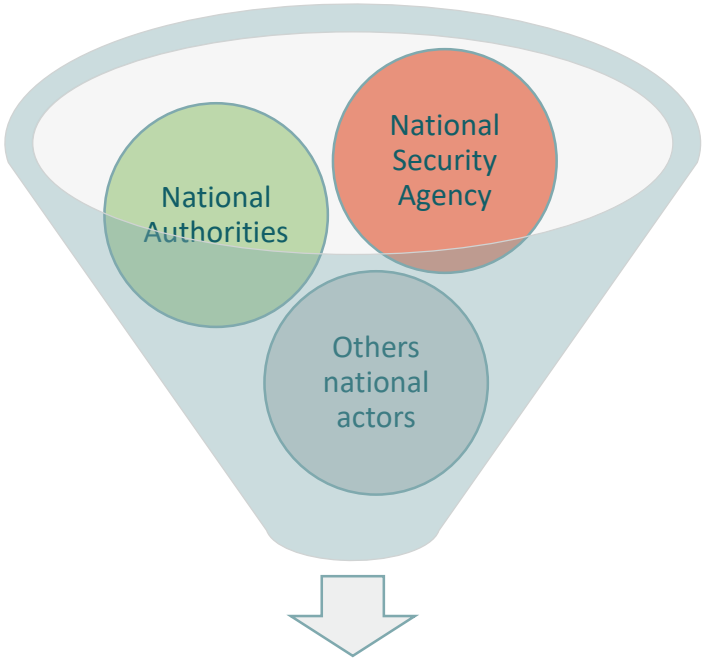
Agenda

- **NIS: within the current framework**
- DORA: the expected evolution
- TIBER-LU: going deeper in cyber resilience test

NIS: within the current framework

Involved players

NIS | DORA | TIBER-LU



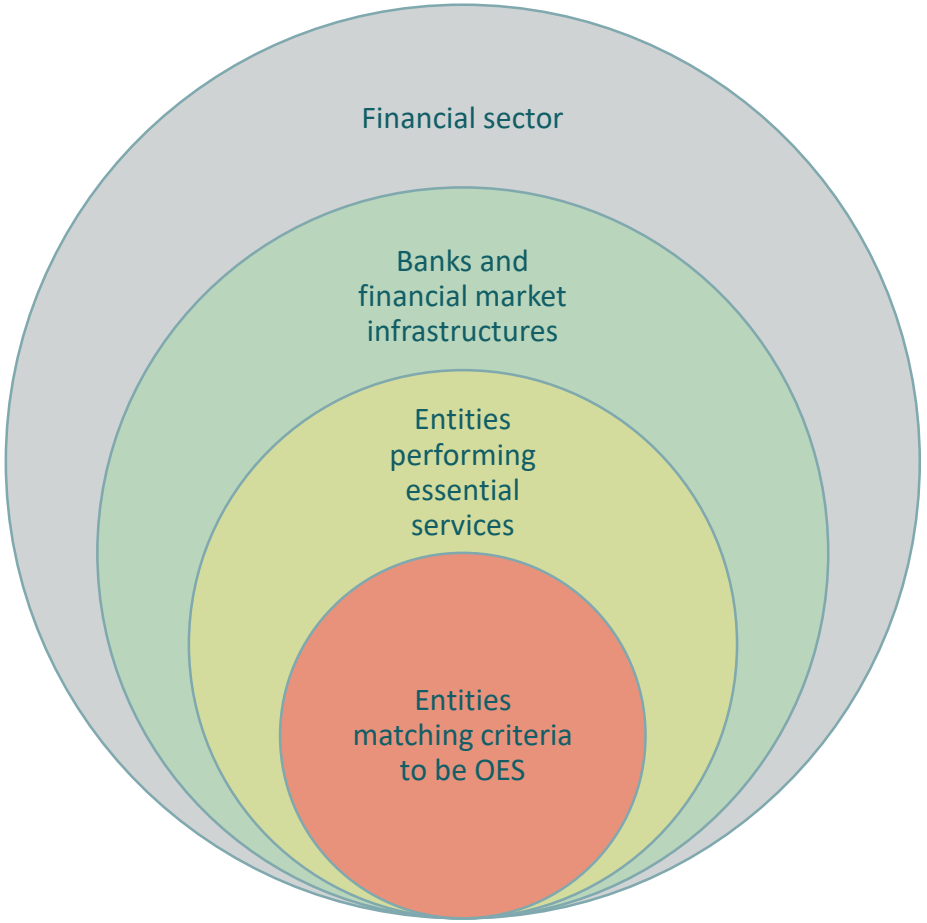
National distribution of roles among agencies and authorities

- In Luxembourg:
  - ILR:
    - NIS authority for all sectors except the Financial Sector (FS) and the Digital Services Providers (DSP) supervised by the CSSF (some Support PFS),
    - LU single point of contact (SPOC)
  - CSSF:
    - NIS authority for FS
    - Incl. support PFS offering cloud computing services, considered as DSP under NIS
  - CIRCL and GOVCERT:
    - Computer Security Incident Response Teams (CSIRTs)
- In the EU: lots of different implementations:
  - Examples of countries where the financial authority is the NIS authority for the financial sector: Netherlands, Ireland, Finland, Austria, Croatia
  - Examples of the opposite: France, Germany, Italy, Czech Republic

NIS: within the current framework

NIS implementation in the financial sector

NIS | DORA | TIBER-LU

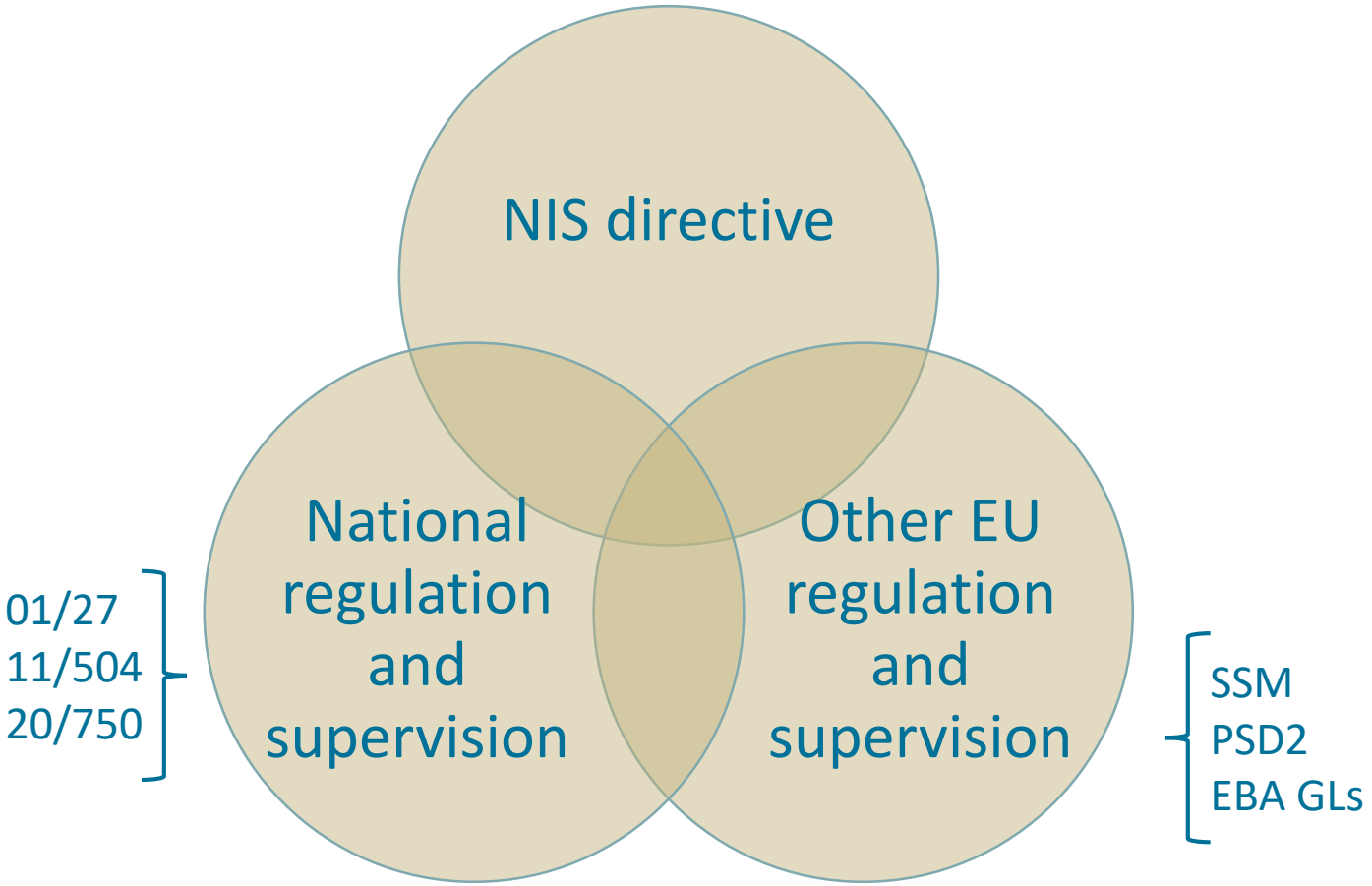


- In Luxembourg, the Law of 28 May 2019 transposes the NIS Directive. Scope for the Financial sector:
  - Banking (credit institutions)
  - Financial Market Infrastructures (operators of trading venue and central counterparties)
- CSSF Regulation N° 20-04: list of essential services
  - Payment services
  - Deposit management
  - Credit granting
  - Investment services
  - Depositary bank
  - Admission of financial instruments to trading on a regulated market trading venue or an MTF
- Among the entities performing these services, a selection has been made by the CSSF based on objective criteria

NIS: within the current framework

Coexistence with existing texts

NIS | DORA | TIBER-LU



- FS was already a high regulated sector at EU and national levels
- Overlaps for OES with regards to
  - Security measures to be implemented
  - Incident reporting
- Particularity for Luxembourg: overlaps on both areas also exist for DSP offering cloud computing services as already supervised by the CSSF as Support PFS
- Lex specialis clause in NIS:
  - To exempt a sector or activity when a EU regulation at least as stringent as NIS applies
  - Valid for payment service providers (PSPs) via PSD2

NIS: within the current framework

Concrete implementation without "reinventing the wheel"

NIS | DORA | TIBER-LU

Measures to manage the risks posed to the security of network and information systems and to prevent and minimise the impact of incidents (OES + DSP)	Notification of those measures to the CSSF (OES only)	Notification of incidents to the CSSF (OES + DSP)
EBA Guidelines on ICT and security risk management	Circular CSSF 01/27	Criteria in NIS Law + Commission Implementing regulation (EU) 2018/151 (for DSP only)
Circular CSSF 20/750 covering OES and DSP [+ Commission Implementing regulation (EU) 2018/151 for DSP only ➔ content is part of circular 20/750]	Long Form Report (+ other existing supervisory tools e.g. IT SREP questionnaire)	Letter to OSE and DSP with minimal information to send and contact details

NIS: within the current framework
Impacts of NIS2

- Expected impacts of NIS2 (draft) on the financial sector:
  - Definition of essential or important entities are embedded into the directive, therefore:
    - No need to define essential services anymore
    - No need to designate OES anymore
    - Enlarged scope for banks and financial market infrastructures
  - More Support PFS may be designed as DSP:
    - "Data centre service providers", in addition to "cloud computing service providers" already in NIS1
    - Other types are currently being discussed

Agenda

- NIS: within the current framework
- **DORA: the expected evolution**
- TIBER-LU: going deeper in cyber resilience test

DORA: the expected evolution

Scope and lex specialis clause

- DORA: Digital Operational Resilience Act
- Ambitious objective: to develop a **single regulatory and supervisory rulebook** for ICT operational resilience in the financial sector (EU regulation + RTS)
- Large scope: **20 types** of regulated Union financial entities
  - All the entities supervised by the CSSF
  - Except Support PFS performing IT operations services
- DORA is intended to be Lex Specialis for the financial entities under the NIS directive
  - The financial entities will apply DORA, instead of the NIS directive, for the **security measures** and the **incident reporting**
  - Other requirements still apply, like information sharing among entities
  - **Lex specialis clause is not applicable to Support PFS**
    - ➔ NIS directive fully applicable to the Support PFS falling under NIS
    - ➔ Overlap between EU and Luxembourg Financial Sector regulation will remain

DORA: the expected evolution
Content and timing

NIS | DORA | TIBER-LU

- Content:
  - **Strong requirements** for the financial institutions on **ICT governance** and **ICT risk management**
  - **Harmonization of incident reporting** from financial institutions to authorities
  - **Third-party risk management** and creation of an **EU Oversight Framework**, for the oversight of Critical ICT Third-Party Service Providers (CTPP)
    - ➔ Some CTPPs (ex. large cloud service providers) may be under national NIS supervision and DORA oversight, at the same time
  - **Resilience testing program** up to mandatory "**Threat-Led Penetration Testing**" (TLPT) for entities designated by the NCAs
- Timing:
  - Entry into force: probably Q4 2022
  - Entry into application: not fully fixed yet, between 12 and 36 months after the entry into force, depending on the requirements

DORA: the expected evolution

Pan-European systemic cyber incident coordination framework

NIS | DORA | TIBER-LU

- On 2 December 2021, the European Systemic Risk Board (ESRB) published a recommendation on a **pan-European systemic cyber incident coordination framework** (EU-SCICF) for relevant authorities
- Triggers:
  - Amount of cyber incidents keeps increasing (+54% between 2019 and 2020, based on the reports provided to ECB Banking Supervision)
  - Large scale incidents call for an effective response from the relevant authorities
  - The risk of coordination failure between authorities exist, potentially leading to inconsistent actions
- Key objective: enable an **effective Union-level coordinated response** in the event of a major cross-border ICT related incident or related threat having a systemic impact on the Union's financial sector as a whole
- The EU-SCICF **anticipates DORA's requirements** and should consider already existing cooperation groups (ex. NIS Cooperation Group)
- Actors involved: ESAs, ECB, ESRB and NCAs
- Timing: gradual implementation, between 30 June 2023 and 31 December 2025 (or between 6 months and 3 years after the entry into force of DORA)

Agenda

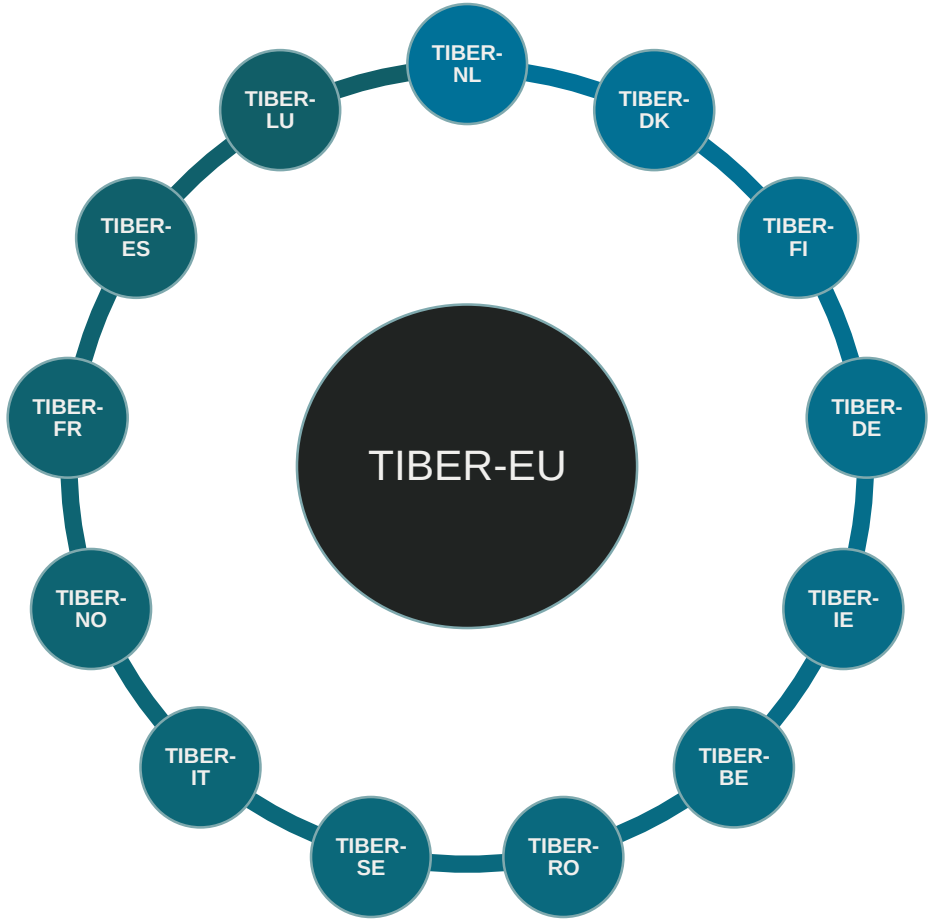
- NIS: within the current framework
- DORA: the expected evolution
- **TIBER-LU: going deeper in cyber resilience test**

TIBER-LU: going deeper in cyber resilience test

What is TIBER-LU?

NIS → DORA → TIBER-LU

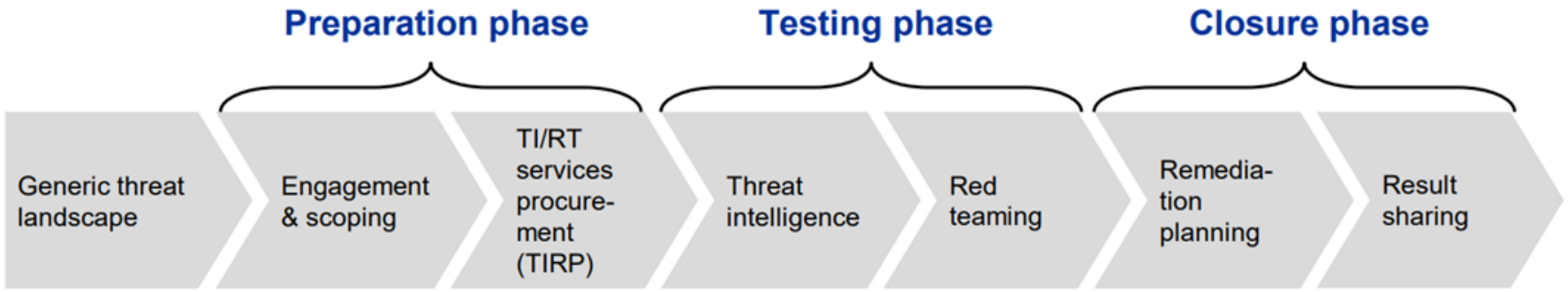
- TIBER = Threat Intelligence-based Ethical Red Teaming
- The BCL and the CSSF jointly adopted the TIBER-LU framework on 3 November 2021
- TIBER-LU is the local implementation of TIBER-EU
- TIBER-EU framework: a harmonized European approach for the conduct of **threat-led penetration tests that mimic the tactics, techniques and procedures of real-life threat actors** and that **simulate a cyber-attack** on critical functions and underlying systems of an entity
- Objectives
  - i) **testing the resilience** of financial markets' entities
  - ii) **facilitating tests for cross-border entities** that are subject to the supervision by several authorities
  - iii) **helping entities** to better assess their protection, detection and response capabilities and to fight against cyber-attacks
- TIBER-LU is **not** a "pass-or-fail" exercise and it is **not** a supervisory tool
- Tests done on **production environment**
- Red team and threat intelligence tests are performed by **external providers**



TIBER-LU: going deeper in cyber resilience test
Global process

NIS → DORA → TIBER-LU

- ~150 MDs for TI and RT providers
- Between 6 to 12 months (depending on the tests complexity and scenarios)

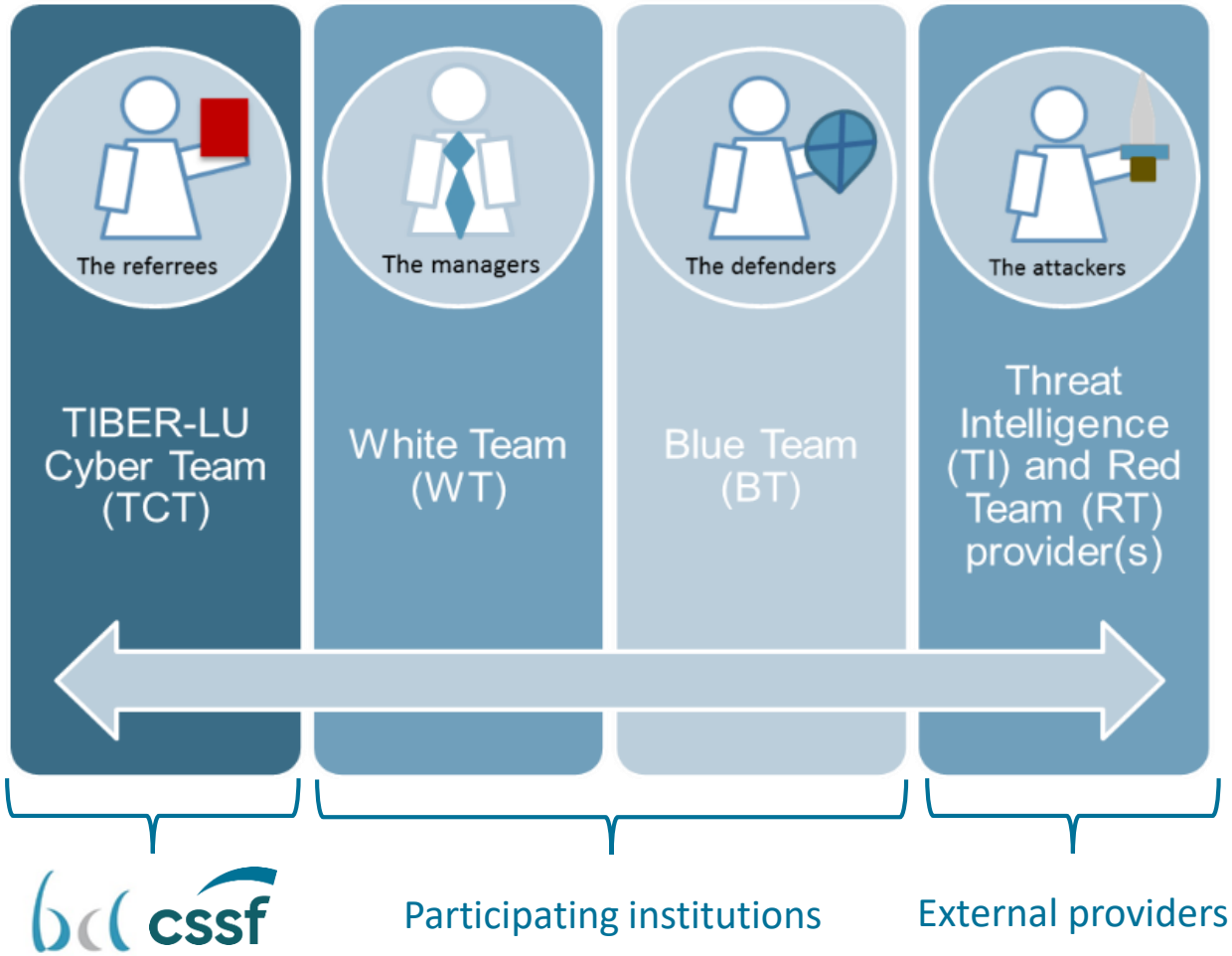


Source: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

- Key outcomes for participating institutions:
  - Targeted TI report and threat scenarios
  - RT test report
  - Remediation plan
  - TIBER-LU test summary
  - Approval and signed certification: obtained from the BCL and the CSSF, attesting that the **test was carried out accordingly to the TIBER-LU framework**

TIBER-LU: going deeper in cyber resilience test
Actors involved

- The direct stakeholders involved in a TIBER-LU test are:
  - The Participating institutions:
    - in which only the **White Team** (WT), led by the White Team Lead (WTL), knows about the test
    - the **Blue Team** (BT) which comprises all staff at the participating entity who are not part of the WT
  - The **TIBER-LU Cyber Team** (TCT) of the BCL and CSSF
  - The third party providers, e.g. **Red Team provider** and the **Threat Intelligence provider**



Conclusion

- Strong will from the EC to **support and harmonise further the cybersecurity posture** in Europe
  ➔ particularly true for the financial sector
- NIS 1/2 and DORA have **strong interactions**
  - This is why lex specialis is possible
  - And makes sense for a highly regulated sector, like the financial sector
- Still, **lex specialis does not mean no coordination and communication**
  - Incident reporting and coordination between the CSSF and the NIS national SPOC (ILR)
  - NIS cooperation group at European level
  - For CTPP, communication between the DORA overseer (called the "Lead Overseer") and the national NIS authority

Thank you for your attention

Questions?