RTS: Threat led penetration tests

Workshop NBS k druhému balíku level 2 regulácie k nariadeniu DORA

NATIONAL BANK OF SLOVAKIA
EUROSYSTEM

Ing. Richard Kellner

11.12.2024 - Kongresová sála NBS

Current state of the RTS

- The ESAs has submitted the final draft RTS to the European Commission for adoption.
- Following its adoption it will be subject to scrutiny of the European Parliament and the Council.
- Afterwards it will be published in the Official Journal of the European Union.
- The expected date of application of these technical standards is

17 January 2025.

Quantitative criteria to perform TLPT

- Credit institutions identified as global systemically important institutions (G-SIIs) or as other systemically important institutions (O-SIIs) or that are part of a G-SIIs or O-SIIs.
- Payment institutions, exceeding EUR 150 billion of payment transactions (2 years)
- Electronic money institutions, exceeding EUR 150 billion of payment transactions (2 years)
- Central securities depositories
- Central counterparties
- Trading venue with the highest market share
- Insurance and reinsurance undertakings with gross written premium (GWP) exceeding EUR 1 500 000 000

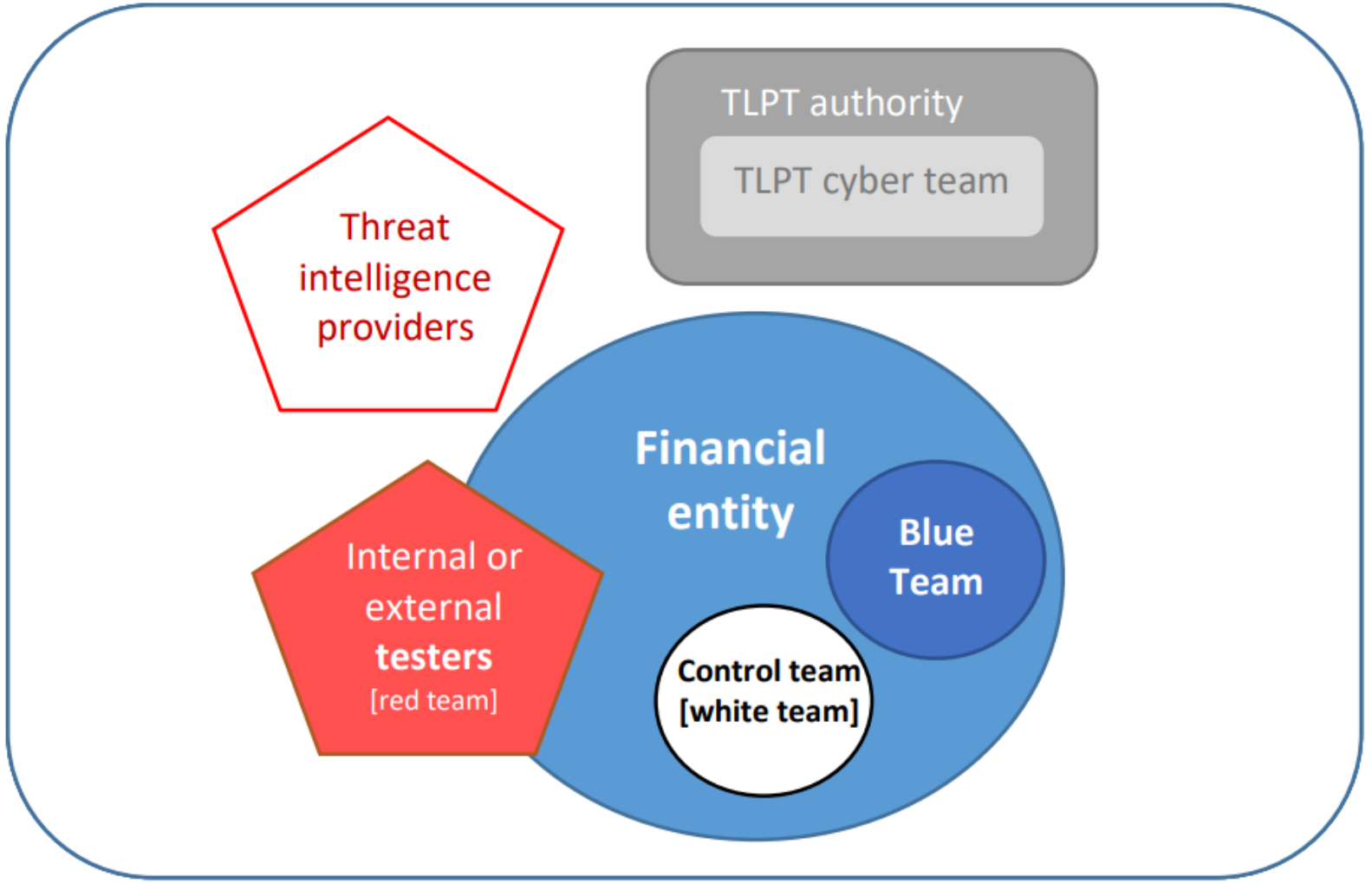
Qualitative criteria to perform TLPT

- Impact-related and systemic character related factors:
  - size of the financial entity
  - extent and nature of the interconnectedness of the financial entity
  - the criticality or importance of the services provided to the financial sector
  - the substitutability of the services provided by the financial entity
  - the complexity of the business model of the financial entity and the related services and processes
  - whether the financial entity is part of a group of systemic character at Union or national level
- ICT risk related factors

TLPT Authority in Slovak Republic

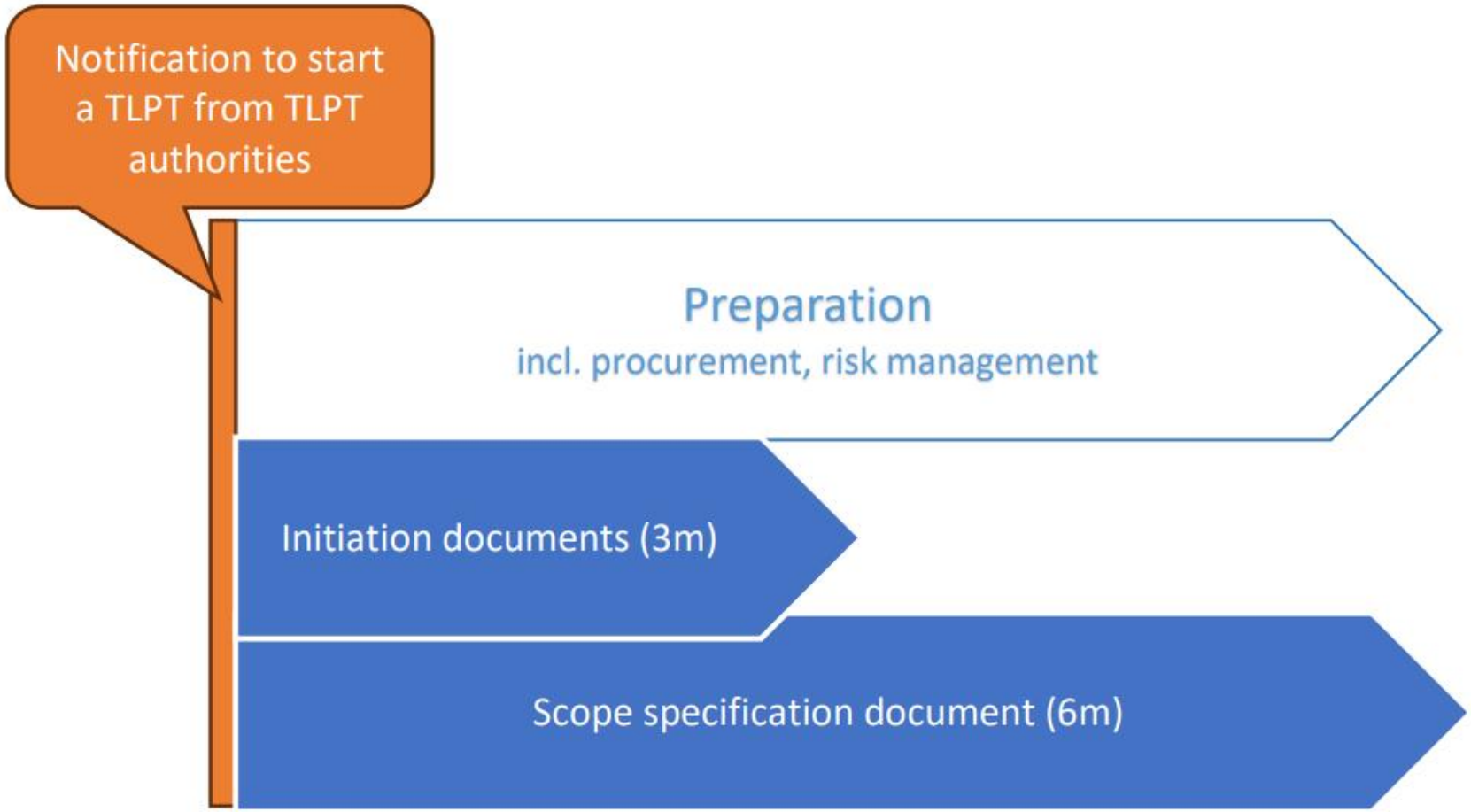
- TLPTA is public authority in the financial sector to be responsible for TLPT-related matters in the financial sector at national level
- **TLPTA in Slovak Republic is NBS**
  - For the purposes of mutual recognition under the DORA, Národná banka Slovenska shall issue attestation of performance a TLPT test.
- **For significant credit institutions (SSM) TLPTA is ECB**
  - Competent authority may delegate the exercise of some or all of the tasks referred to another national authority in the financial sector.

TLPT participants

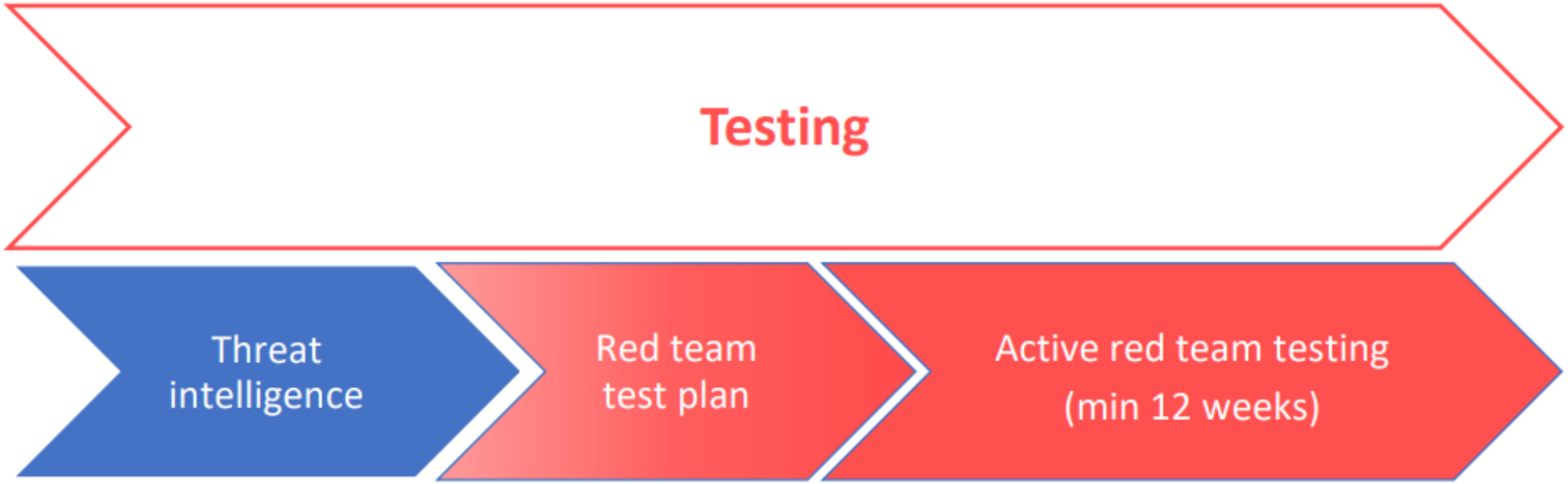


TLPT Phases

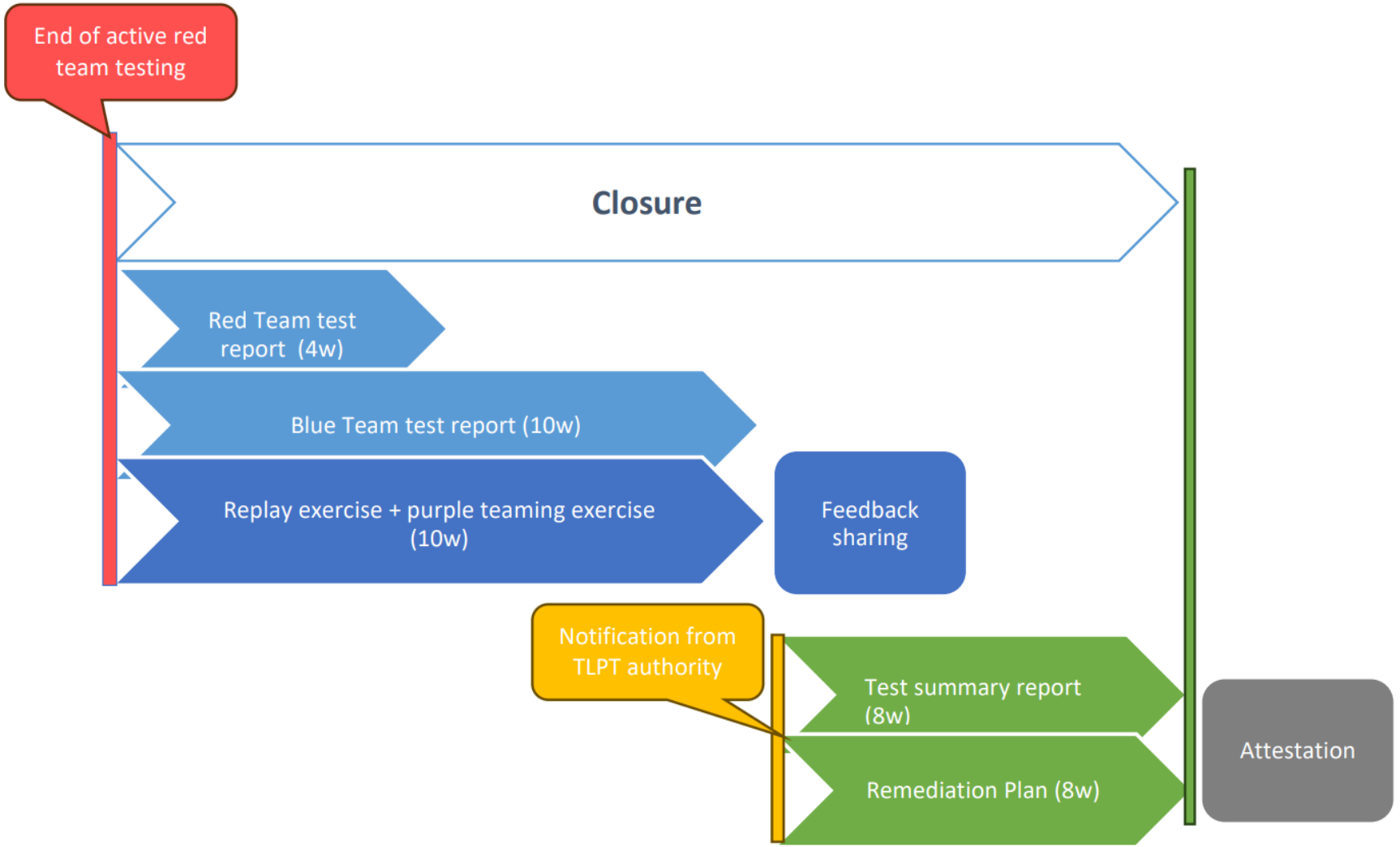
Preparation phase



Testing phase



Closure phase



International TLPTs

- **Joint TLPTs.** Another case for cooperation between TLPT authorities is when TLPT authorities decide to organise joint TLPTs on several financial entities established in different Member States but using the same ICT intra-group service provider, or belonging to the same group and *using common ICT systems*.

- **Pooled TLPTs.** In this case the TLPT authorities shall designate which financial entity shall be the designated financial entity according to Article 26(4) DORA and which financial entities only participate in the pool and once again the TLPT authorities of the pariticipating financial entities shall agree amongst themselves as to who shall lead the TLPT.

TIBER-EU framework

- The TIBER-EU framework aims to harmonize and standardize the approach to threat intelligence-based ethical red-teaming across Europe.

- TIBER-EU framework can also assist competent authorities and financial entities in meeting the requirements for threat-led penetration tests under the Digital Operational Resilience Act (DORA).

- Mutual recognition of TIBER-XX and DORA TLPT (*only if the same group is using common ICT systems*)

Q&A ???

Ďakujem za pozornosť

NATIONAL BANK OF SLOVAKIA
EUROSYSTEM

Ing. Richard Kellner

11.12.2024 - Kongresová sála NBS