From NIS 1 to NIS 2:

What changes to expect for professionals of the financial sector?

17 October 2023

Cécile Gellenoncourt
Head of service line
Supervision of information systems and of Support PFS

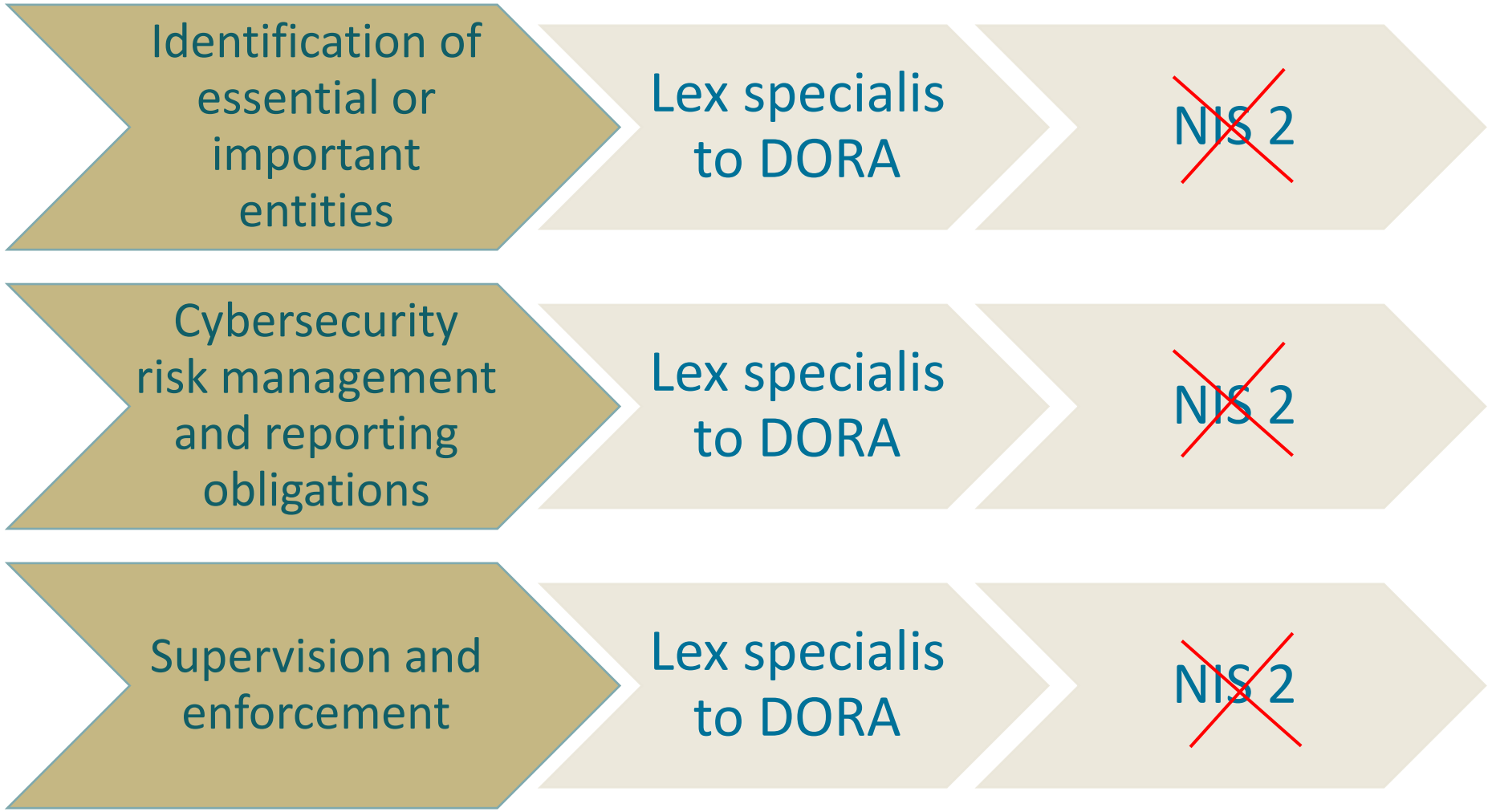
cssf
Commission de Surveillance
du Secteur Financier

Agenda

- **NIS 2 scope for PFS and interaction with DORA**
- Cybersecurity risk-management measures
- Incident reporting

Banking and Financial Market Infrastructures (1/2)

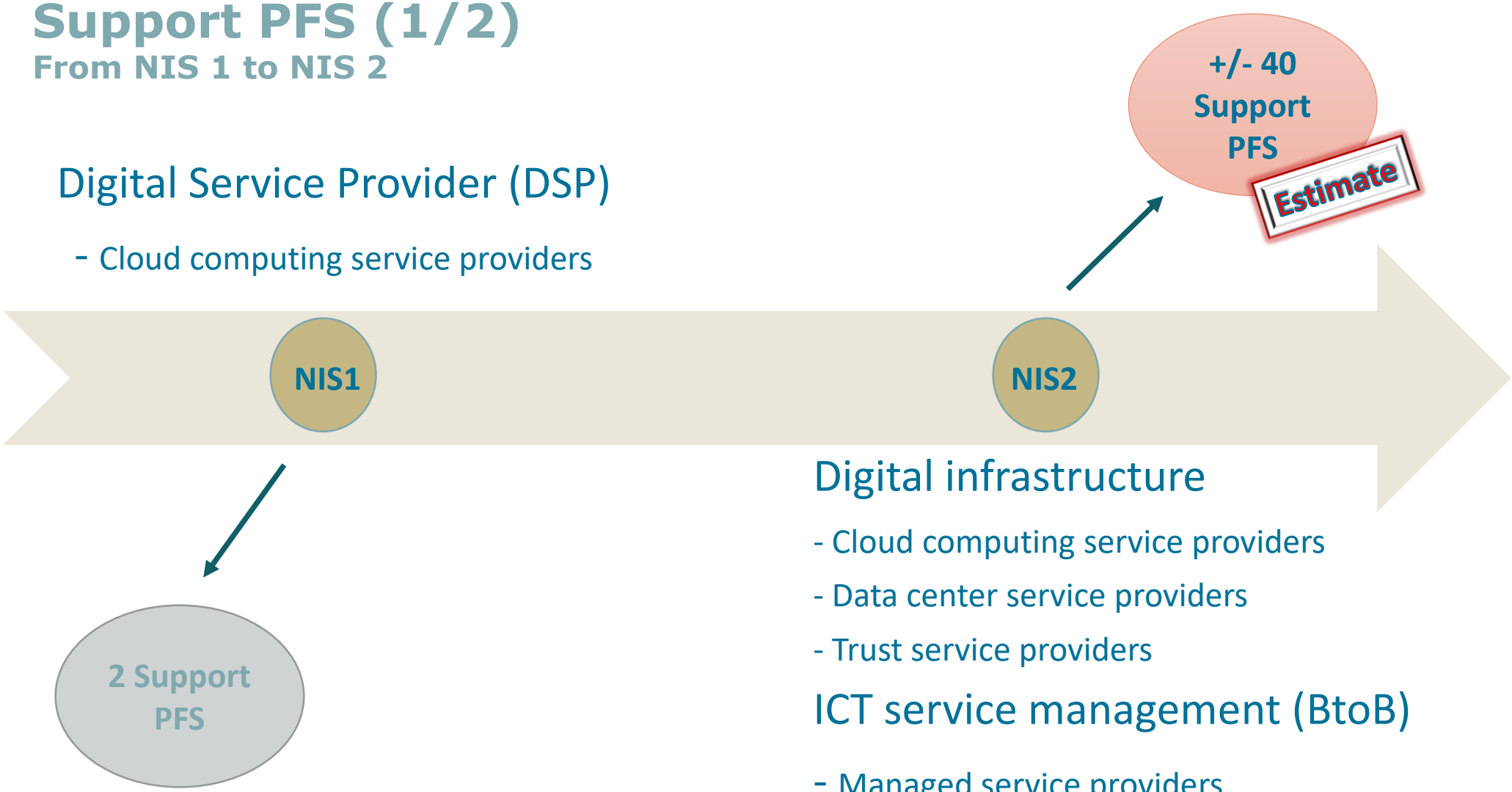
From NIS 1 to NIS 2



Banking and Financial Market Infrastructures (2/2)
From NIS 1 to NIS 2

- Beyond lex specialis rule to DORA, **important NIS2 requirements remain for NIS authorities and Member States:**
  - **Transmission of major ICT-related incidents** under DORA and where relevant, cyber threats to the CSIRTs, the NIS authority (= CSSF), and the NIS2 SPOC
  - **CSIRTs** should be in a position to cover the financial sector in their activities
  - Inclusion of the financial sector in the **national cybersecurity strategy and crisis management framework**
  - The European cyber crisis liaison organisation network (**EU-CyCLONe**) also covers the financial sector
  - **The ESAs and CA under DORA may participate** in the activities of the **NIS Cooperation Group** for matters that concern their supervisory activities in relation to financial entities.

Support PFS (1/2)
From NIS 1 to NIS 2



Digital Service Provider (DSP)

- Cloud computing service providers

Digital infrastructure

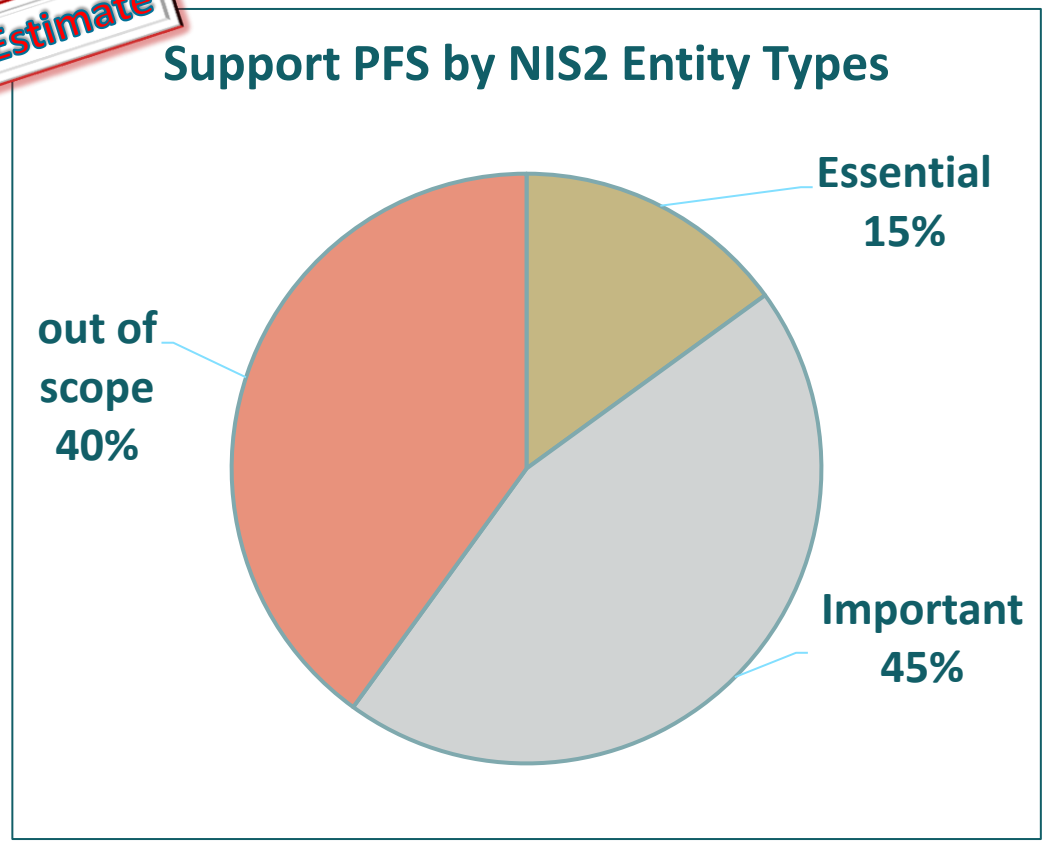
- Cloud computing service providers
- Data center service providers
- Trust service providers

ICT service management (BtoB)

- Managed service providers
- Managed security service providers

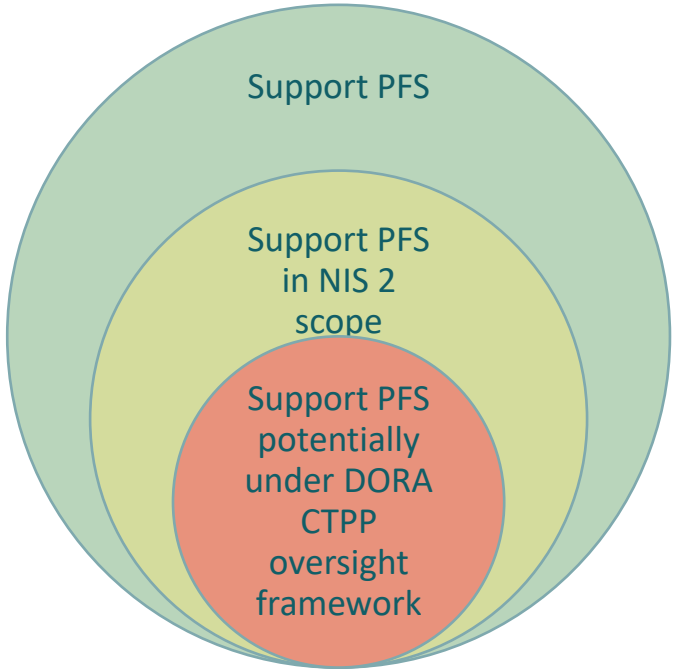
Support PFS (2/2)
From NIS 1 to NIS 2

Estimate

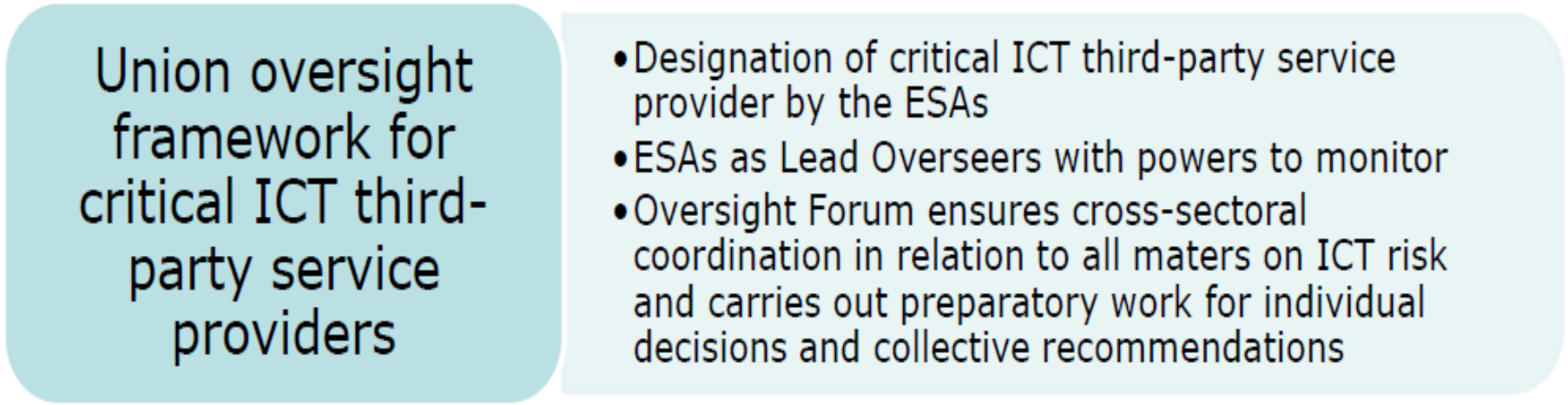


+

Critical Third-Party Providers (CTPP) oversight framework under DORA for a few Support PFS?



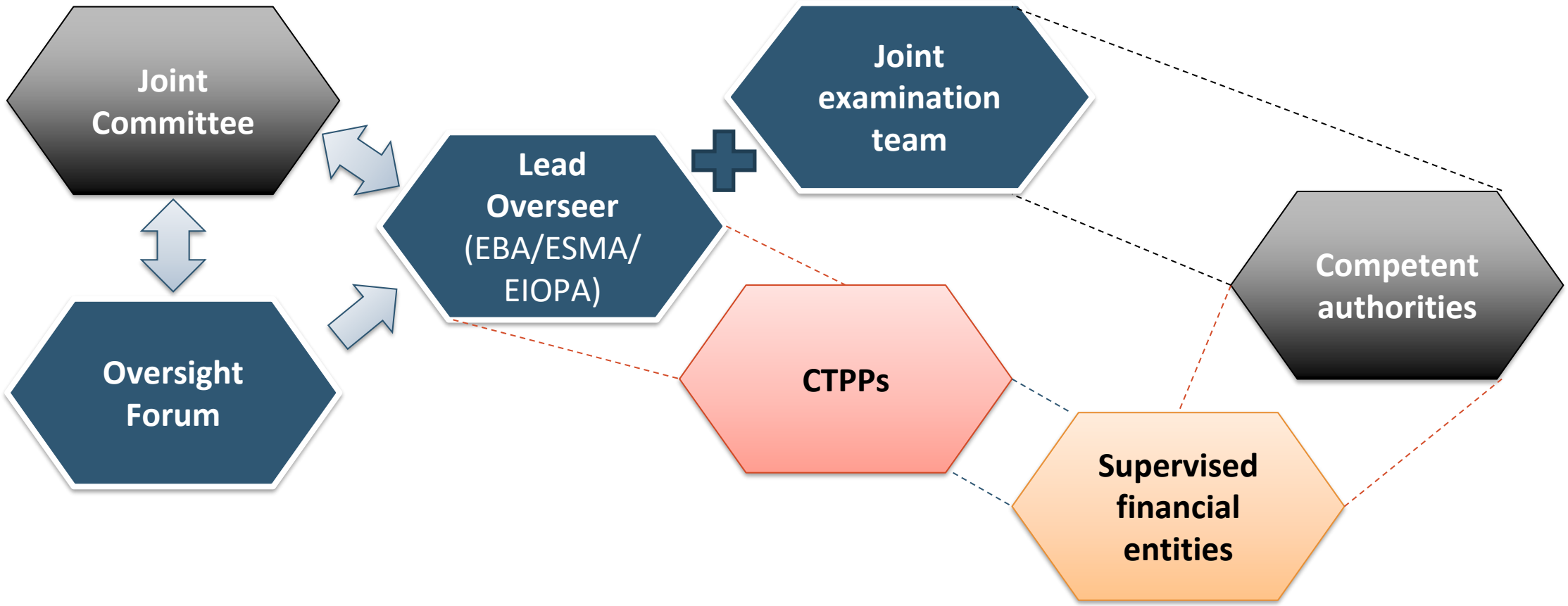
Oversight framework for CTPPs



- Criteria to designate the CTPPs in DORA regulation:
  - Systemic impact on the stability, continuity or quality of the provision of financial services
  - Systemic character/importance of the financial entities that rely on the relevant ICT third-party provider
  - Reliance of FE on the services provided in relation to critical or important functions
  - Degree of substitutability of the ICT third-party service provider
- Criteria to be further specified by a delegated act to be adopted by the EC
- Where the TPP belongs to a group, criteria to be considered in relation to ICT services provided by the group as a whole

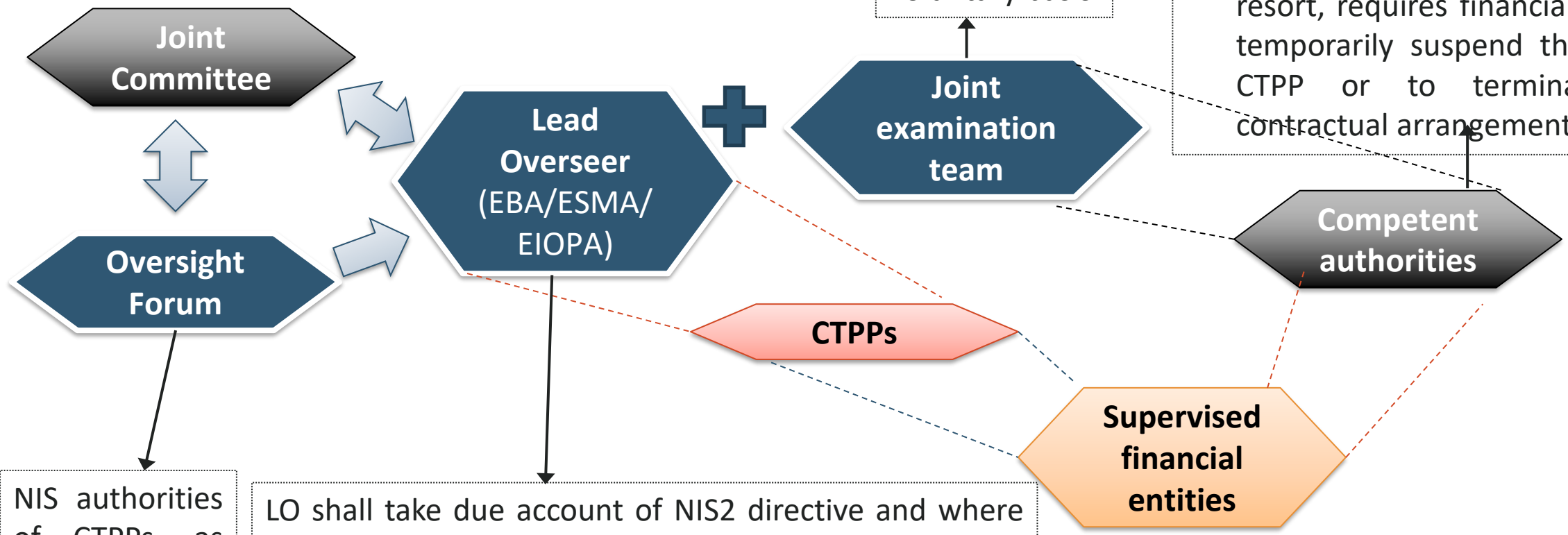
CTPP Oversight framework

Overview of interaction between key stakeholders under DORA



CTPP Oversight framework

Overview of interaction between key stakeholders under DORA and NIS authorities



CTPP's NIS authority as member, on a voluntary basis

A CA may, on a voluntary basis, consult the NIS authority of a CTPP:

1) about the recommendations addressed by the LO to a CTPP, or
2) when the CA, as a measure of last resort, requires financial entities to temporarily suspend the use of a CTPP or to terminate the contractual arrangement.

NIS authorities of CTPPs, as observer

LO shall take due account of NIS2 directive and where necessary, consult the NIS authority to avoid duplication of technical and organisational measures that might apply to CTPP under NIS2

Cooperation between DORA and NIS2 authorities for CTPPS falling under NIS2 (DORA Article 47)

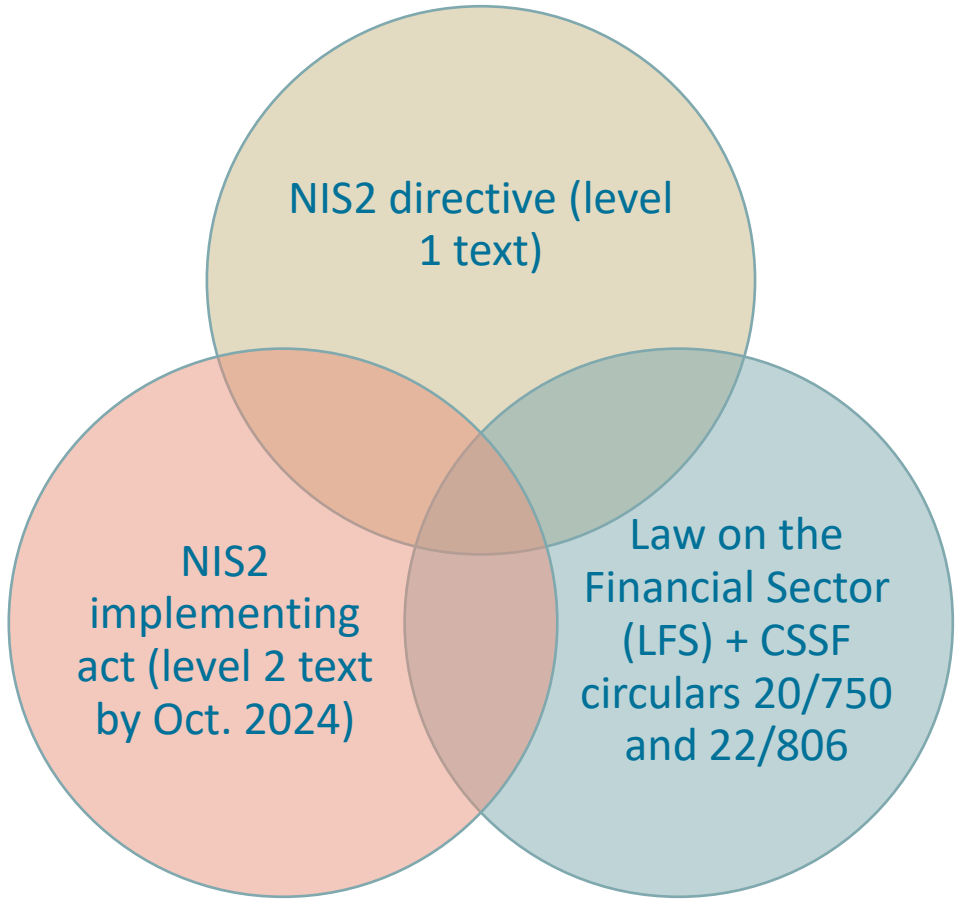
- **The ESAs and CA under DORA may** request to be invited to **participate** in the activities of the **Cooperation Group** for matters in relation to essential or important entities subject to NIS2 that have also been designated as CTPP
- Where appropriate, **competent authorities may establish cooperation arrangements with NIS authorities:**
  - to specify, inter alia, the procedures for the **coordination of supervisory and oversight activities** in relation to essential or important entities subject to NIS 2 that have been designated as CTPP under DORA,
  - including for the conduct, in accordance with national law, of **investigations and on-site inspections,**
  - as well as for mechanisms for the **exchange of information** between the DORA competent authorities and the NIS2 authorities

Agenda

- NIS 2 scope for PFS and interaction with DORA
- **Cybersecurity risk-management measures**
- Incident reporting

Cybersecurity risk management measures

Regulatory requirements



- Strong overlap between NIS2 directive requirements and FS requirements.

  However,

  - Some gaps notably on supply chain risk
  - Assessment to be confirmed when NIS2 implementing act is final

- This means that compliance with CSSF circular 20/750 on ICT and security risk management and 22/806 on outsourcing is a good signal for compliance with NIS2 requirements.

  However,

  - On-site inspections sometimes reveal areas for improvement or weaknesses…
  - So do not wait to perform a compliance check / gap analysis with 20/750 and 22/806 requirements and take actions as relevant

Cybersecurity risk management

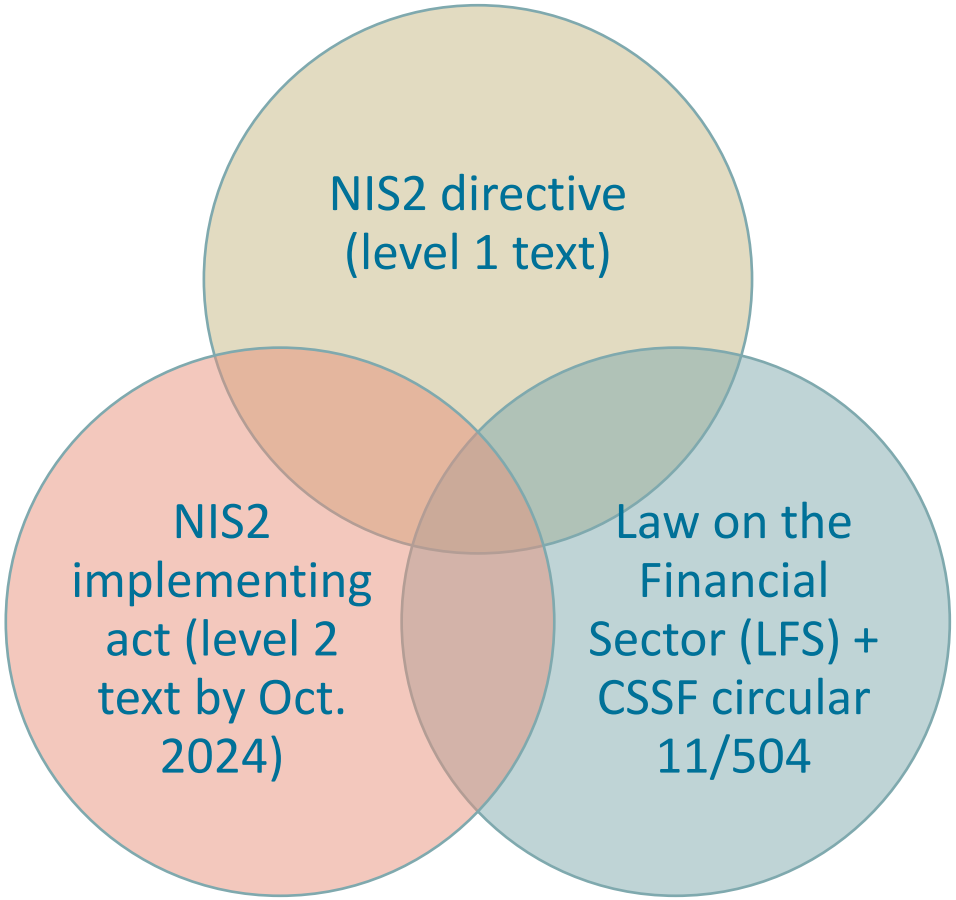
Necessary adaptation of CSSF circulars and supervision tools

Cybersecurity risk management requirements	Annual reporting to the CSSF	Other supervision tools
Circulars CSSF 20/750 and 22/806…	Current descriptive report, risk assessment report and mandate to audit firms…	Outsourcing authorisation or notification, new service review, on-site inspections, etc.
To be adapted, where relevant, to avoid repetition and ensure good articulation with NIS 2 texts.	To be replaced by Self Assessment Questionnaire (SAQ) and more precise guidance to audit firms on the tests to be performed	Globally unchanged but taking NIS2 level 2 text on board. Potential use of new tools (e.g. security scans) under consideration

Agenda

- NIS 2 scope for PFS and interaction with DORA
- Cybersecurity risk-management measures
- **Incident reporting**

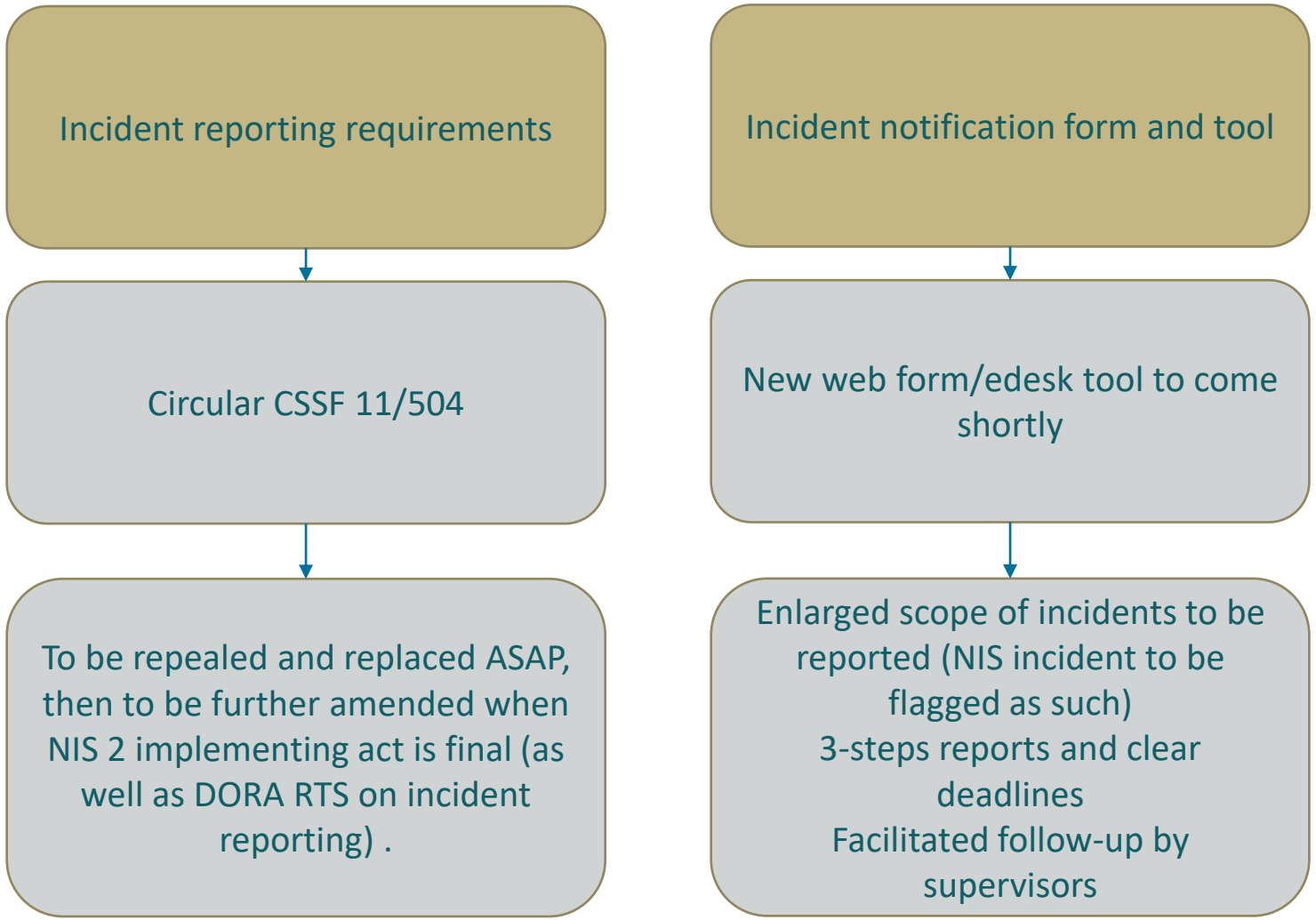
Incident reporting
Regulatory requirements



- Partial overlap between NIS2 directive requirements and FS requirements. Gaps exist:
  - Differences in scope of incidents to be reported
  - no initial, intermediate, final reports
  - No deadlines clearly specified
  - …
- Gaps to be expected as higher when NIS2 implementing act is final
- Need to review Circular CSSF 11/504 on frauds and external computer attacks

Incident reporting

Necessary adaptation of CSSF circulars and supervision tools



Thank you for your attention

Questions?