DIGITAL OPERATIONAL RESILIENCE ACT (DORA) - REPORTING OF REGISTER OF INFORMATION, OF MAJOR ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS - UPDATE

BACKGROUND

- The **Digital Operational Resilience Act** (DORA) was published in the Official Journal of the European Union **entered into force on 16 January 2023** and **will apply from 17 January 2025**.
- DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to **20 different types of financial entities**, including insurance and reinsurance undertakings, IORPs and insurance and reinsurance intermediaries.
- **DORA is *lex specialis* to** the Network Information Security (**NIS**) **Directive** and to Article 11 and Chapters III, IV and VI of the Critical Entity Resilience (**CER**) **Directive**.
- To operationalise its application, DORA mandates the European Supervisory Authorities (**ESAs**) **to prepare jointly**, through the Joint Committee (JC), **a set of policy products** with two main submission deadlines 17 January 2024 (first batch) and 17 July 2024 (second batch)

THE PILLARS OF DORA

ICT risk management	ICT 3rd party risk management	Digital operational resilience testing	ICT-related incidents	Information Sharing	CTPP oversight
▪ Principles and requirements on ICT risk management framework	▪ Monitoring third-party risk providers ▪ Key contractual provisions ▪ Register of information on ICT third-party providers	▪ Basic testing ▪ Advanced testing	▪ General requirements ▪ Reporting of major ICT-related incidents to competent authorities	▪ Exchange of information and intelligence on cyber threats	▪ Oversight framework for critical ICT TPPs

DORA POLICY MANDATES AN OVERVIEW

ICT risk framework (Chapter II)

- RTS on ICT Risk Management framework (Art.15)
- RTS on simplified risk management framework (Art.16.3)
- Guidelines on the estimation of aggregated costs/losses caused by major ICT related incidents (Art. 11.1)

ICT related incident management classification and reporting (Chapter III)

- **RTS on criteria for the classification of ICT related incidents (Art. 18.3)**
- **RTS to specify the reporting of major ICT-related incidents (Art. 20.a)**
- **ITS to establish the reporting details for major ICT related incidents (Art. 20.b)**
- Feasibility report on further centralisation of incident reporting through the establishment of a single EU hub for major ICT-related incident reporting (Art. 21)

Digital Operational Resilience Testing (Chapter IV)

- RTS to specify threat led penetration testing (Art. 26.1)

Third-party risk management (Chapter V.I)

- **ITS to establish the templates of register of information (Art.28.9)**
- RTS to specify the policy on ICT services performed by third-party (Art.28.10)
- RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5)

Oversight framework (Chapter V.II)

- Call for advice on criticality criteria (Art. 31.8) and fees (Art. 43.2)
- Guidelines on “CAs-ESAs cooperation” regarding DORA oversight (Art. 32.7)
- RTS on “oversight conduct” (Art. 41)

Bold = mandates with impacts on reporting for financial entities

REGISTER OF INFORMATION

- Article 28(3) of **DORA introduces the requirements for all financial entities to maintain and update a register of information on all their ICT third-party arrangements** at entity, sub-consolidated and consolidated level.
- According to Article 31(10) **the register of information should constitute the key source of information to designate ICT third-party service providers** to the financial sector as critical (CTPPs) and therefore include them in the scope of DORA oversight.
- To apply the criteria included in DORA to designate the CTPPs, **the ESAs will need to receive the full register of information to be collected by CAs from their respective financial entities**.
- The **templates of the register of information are formalised in an ITS which has been publicly consulted with the stakeholders between 19 June and 11 September 2023**. Cross-sectoral, the ESAs have received 95 replies on the public consultation paper.
- The **final report on the public consultation paper and the ITS are due by 17 January 2024**.

STRUCTURE OF THE CONSULTED REGISTER OF INFORMATION

Illustration 1: Structure of the Register of Information maintained and updated at entity level

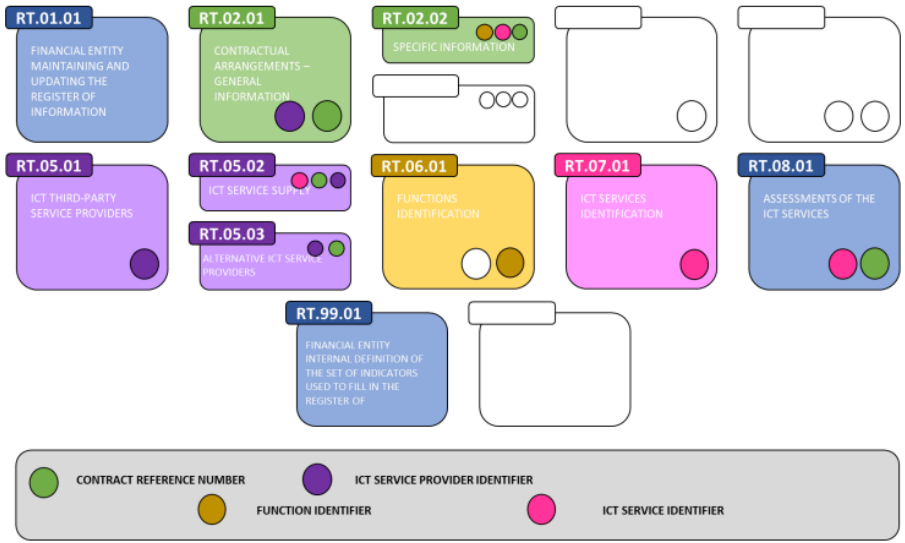
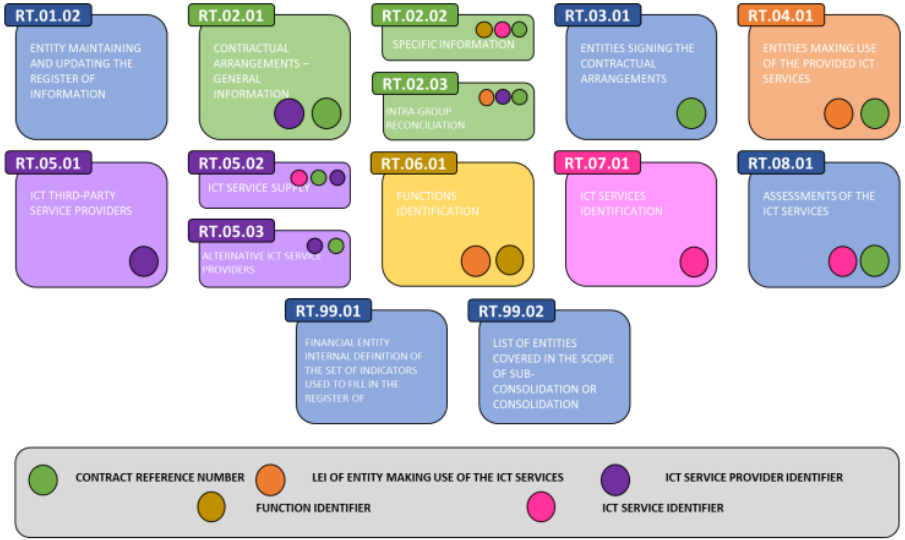
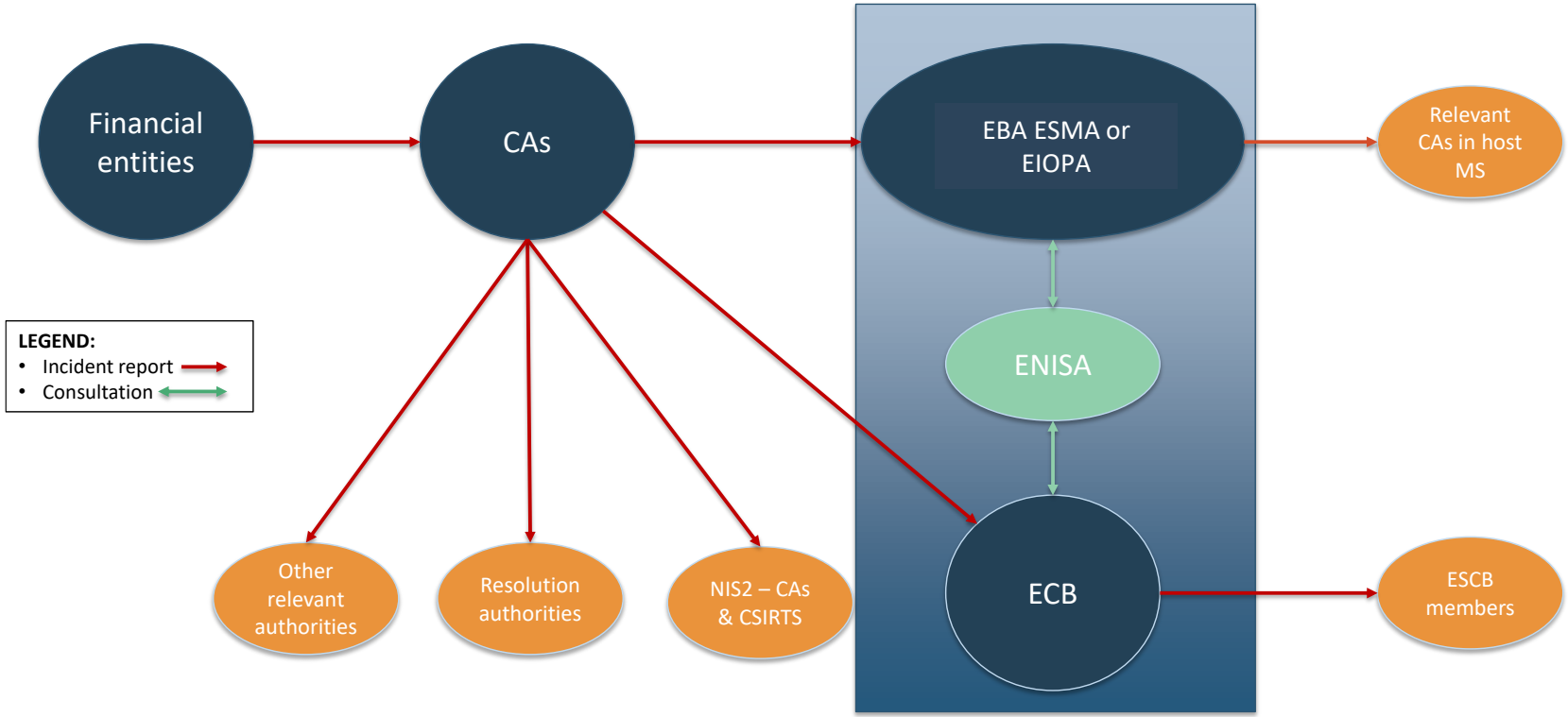


Illustration 2: Structure of the register of information at (sub)consolidated level



MAJOR ICT RELATED INCIDENT REPORTING ILLUSTRATIVE OVERVIEW OF THE REPORTING FLOW EX ARTICLE 19

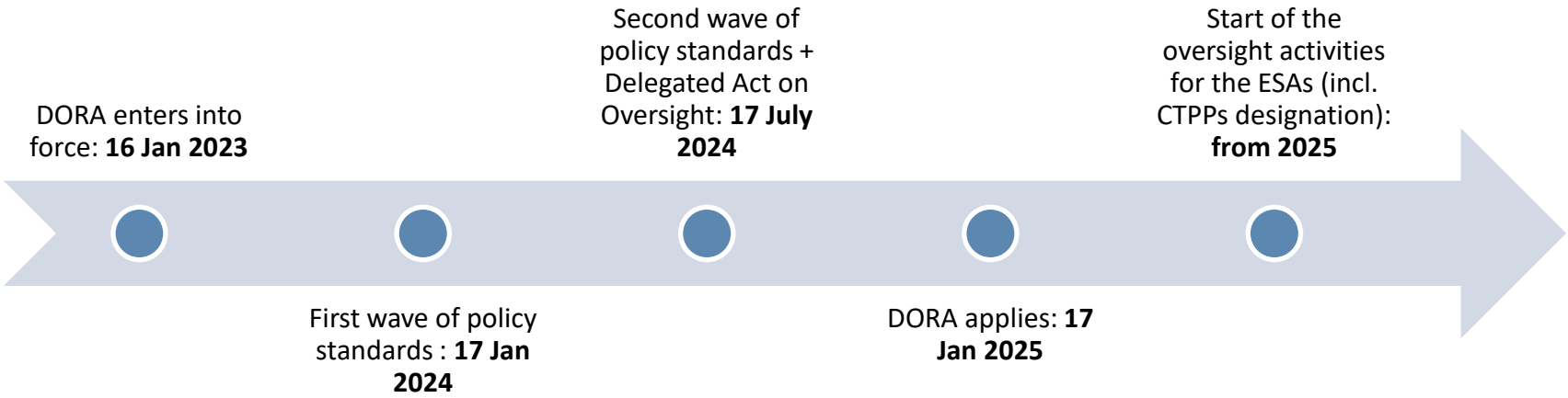


OBLIGATIONS FOR FINANCIAL ENTITIES AND L2 STATUS UPDATE

- **Article 19** of DORA **introduces the requirement for all financial entities to report to the relevant CA**
  - **major ICT-related incidents**. The reporting shall be composed by an Initial notification*; interim report(s) and a final report
  - **on a voluntary basis, significant cyber threats***
- The **draft RTS** on **criteria and materiality thresholds** determining major ICT related incidents and significant cyber threats and the criteria to be applied by CAs to assess cross-border nature of an incident and the details to be shared with CAs from other MS were **publicly consulted with the stakeholders between 19 June and 11 September 2023**. Cross-sectoral, the ESAs have received 103 replies on the public consultation paper. The **final report on the public consultation paper and the RTS are due by 17 January 2024**.
- The ESAs are also working on a **draft ITS and a draft RTS to harmonise reporting content and templates**. Those draft TS will be **publicly consulted for 3 months from Nov/Dec 2023**.

* Upon MS determination, FEs (1) shall transmit the initial notification and (2) may transmit the notification on cyber threats to the Computer Security Incident Response Teams CSIRTs

SUMMARY: OVERALL TIMELINE FOR DORA IMPLEMENTATION



THANK YOU!

For more information visit:
https://www.eiopa.europa.eu