Implementation of DORA. Reporting requirements

Oleg SHMELJOV | Senior Policy Expert, European Banking Authority

06 June 2024 | Eurofiling Conference, Dublin

eba European Banking Authority

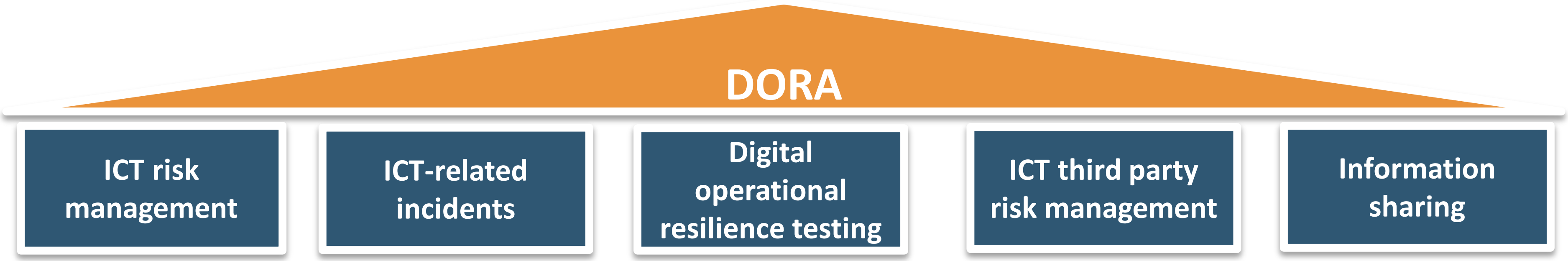
eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

Digital Operational Resilience Act (DORA)

DORA establishes a comprehensive framework for digital operational resilience for financial entities (FEs) in the EU. This is to address (i) dependency of the financial sector on technology companies and (ii) cyber risks and other vulnerabilities of FEs

DORA entered into force on 16 Jan 2023 and will start applying from 17 Jan 2025



DORA

ICT risk management

- Principles and requirements on harmonised **ICT risk management** framework

ICT-related incidents

- Harmonised **ICT-related incident management, classification and reporting** requirements

Digital operational resilience testing

- **Coordinated testing** and mutual recognition of **advanced testing** for significant financial entities

ICT third party risk management

- Monitoring third-party risks, key contractual provisions and establishment of **oversight framework for CTPPs**

Information sharing

- Exchange of information and **intelligence on cyber threats**

DORA:

- Strengthens ICT risk management and third-party risk management in FEs
- Enhances supervision of ICT risk management,
- Introduces oversight of critical ICT third-party service providers (CTPPs)

Entities within scope: wide range of FEs (21 different types) from banking, investment and insurance sectors, as well as ICT third-party service providers.

eba European Banking Authority

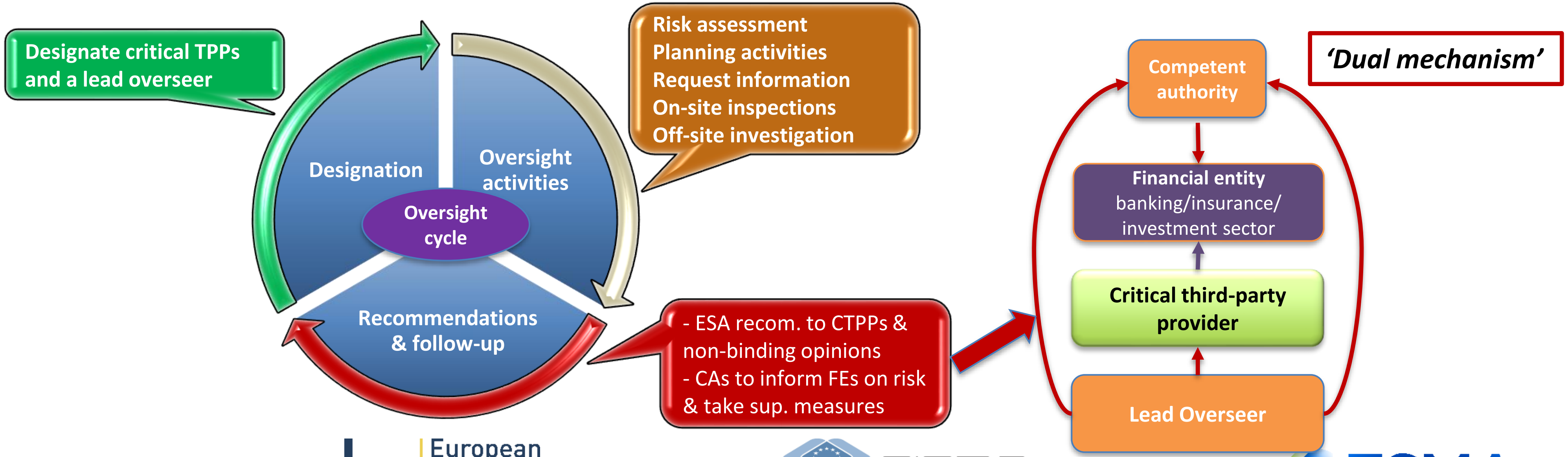
eiopa European Insurance and Occupational Pensions Authority

ESMA European Securities and Markets Authority

DORA oversight of critical ICT third-party service providers

Features of the oversight framework

- ESAs to assess if CTPPs have in place adequate processes to manage the risks they may pose to financial entities (FEs)
- Lead Overseer can issue recommendations to the CTPPs following general investigations or onsite inspections
- Competent authorities may follow-up on the recommandations of the Lead Overseer by requiring the FEs they supervise to take measures to address these risks
- ESAs and competent authorities cooperate closely in the designation and day-to-day oversight of the CTTPs
- CTPP oversight will be funded by the oversight fees, but the oversight set-up should be covered by the ESAs general existing budget
- DORA builds on the existing institutional supervisory architecture in the financial sector enhanced by new structures (Oversight Forum, Joint Oversight Network, Joint Examination Teams)
- Close coordination across sectors and cooperation between ESAs, CAs and other EU institutions/agencies



Designate critical TPPs and a lead overseer

Risk assessment
Planning activities
Request information
On-site inspections
Off-site investigation

- ESA recom. to CTPPs & non-binding opinions
- CAs to inform FEs on risk & take sup. measures

'Dual mechanism'

Designation
Oversight activities
Oversight cycle
Recommendations & follow-up
Competent authority
Financial entity banking/insurance/ investment sector
Critical third-party provider
Lead Overseer

eba European Banking Authority

eiopa European Insurance and Occupational Pensions Authority

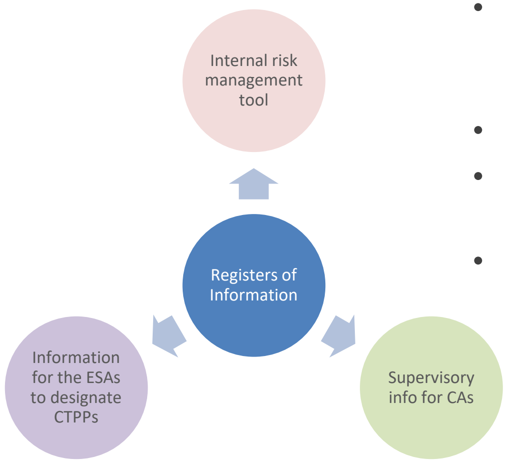
ESMA European Securities and Markets Authority

DORA reporting obligations

- New reporting obligations for financial entities:
  1. Annual reporting of registers of information of contractual arrangements with ICT third-party service providers
  2. Notification and reporting of major incidents and significant cyber threats
- No standardised regular reporting from ICT third-party service providers → information requests for the oversight activities

Reporting of registers of information

- DORA requires all FEs in its scope to have a register of information of all their contractual arrangements with ICT third-party providers available at entity, sub-consolidated and consolidated levels
- FEs will need to report the registers of information to the competent authorities starting from early 2025
- CAs will provide the registers on annual basis to the ESAs for the purposes of designation of CTPPs

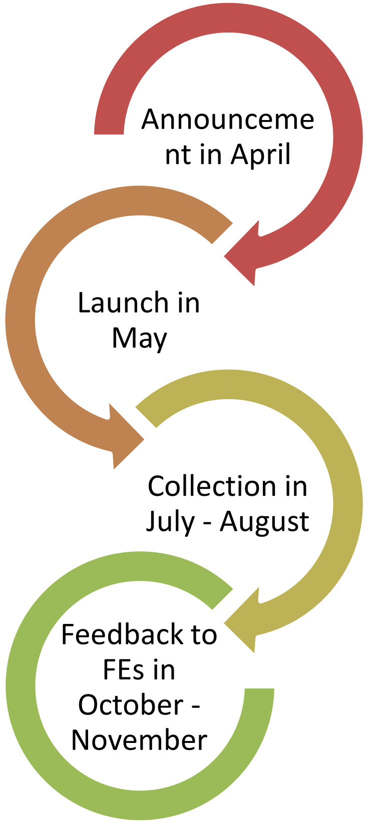

Internal risk management tool
Registers of Information
Information for the ESAs to designate CTPPs
Supervisory info for CAs

- Structure of the registers and data fields are set out in the dedicated implementing technical standards (ITS)
- Annual reporting of complete registers
- Reporting supported by the data point model, taxonomy and validation rules
- Simplified reporting format – plain-csv

Reporting of incidents

- DORA requires all FEs in its scope to have in place ICT-related incident management process that includes inter alia recording of all ICT incidents and significant cyber threats, and reporting of major incidents to the authorities → requires assessment and classification of incidents
- FEs must report all major ICT-related incidents to the relevant competent authorities. Three-staged reporting process:
  - Initial notification
  - Intermediate report
  - Final report
- Notification of significant cyber threats is voluntary
- Classification of incidents and their reporting is done based on the requirements set out in relevant regulatory and implementing technical standards (RTS & ITS)
- CAs use the reports for their supervisory purposes and forward them to the ESAs (and other relevant authorities) → ESAs analyse and disseminate the information to other authorities affected by the incident
- Possible future centralisation of reporting via a single EU Hub → dedicated mandated for a feasibility study

2024 Dry run exercise on reporting of registers of information


Announcement in April
Launch in May
Collection in July - August
Feedback to FEs in October - November

Objectives of dry run exercise

- Help with the preparations for establishing and reporting registers of information by the financial entities and competent authorities
- Take stock of the preparedness of the market and increase awareness
- Help with the preparation of the reporting files
- Identify and address data quality concerns

Key milestones:

- **11 April** – Publicly communication about the ad-hoc data collection
- **30 April** – Introductory workshop for the industry
- **31 May** – Launch for the industry: materials, specifications and tools made available to the participating FEs
- **June-July** – ESAs' workshops with participating FEs and competent authorities; FAQ support → 10 June workshop for industry to introduce the tools
- **1 July-30 August** – registers of information collected (no resubmissions envisaged) from participating FEs through their competent authorities (which may set specific deadlines within this window)
- **31 October** – end of the data analysis and quality checks. Feedback to be provided to the participating FEs via their competent authorities
- **November** – ESAs' 'lessons learnt' workshop on data quality open to the entire industry
- **Early December** – publication of aggregated data quality report