Navigating the Digital Operational Resilience Act (DORA)

22 May 2025, 11th International Compliance Forum (Limassol, Cyprus)

Andreas Papaetis
Senior Policy Expert

Digital Operational Resilience Act (1)

'Genesis' of DORA

Situation

- **Growing reliance of the EU financial sector on ICT services**, resulting in making the EU financial sector vulnerable to problems with underlying tech.
- **Significant rise in cyber incidents and threats** (with ransomware and DDoS attacks being the most prevalent threats), often exploited vulnerabilities in third-party service providers and supply chains.
- **ICT risks *partially* addressed at EU level**:
  - General rules: partial application finance, unevenly implemented
  - Financial services rules: patchy, inconsistent, fragmented

Reaction

- ✓ ***April 2019:*** *The ESAs jointly issued technical advice calling for a coherent approach to ICT risk in finance and recommending to strengthen the digital operational resilience through a sector–specific initiative.*
- ✓ ***September 2020:*** *The European Commission proposed a new legislation for an EU regulatory framework on digital operational resilience (DORA), a dedicated framework to safeguard digital operational resilience for finance.*
- ✓ ***January 2023:*** *DORA enters into force.*
- ✓ ***January 2025:*** *DORA enters into application.*

Digital Operational Resilience Act (2)

Aim, objectives and expected benefits

Aim: consolidate and upgrade ICT risk requirements throughout the EU financial sector to guarantee a homogenous and coherent application of all components of ICT risk management -> **Upgrade EU rules to promote resilience**

Objectives and expected benefits

- ***One set of common rules across the EU*** reducing compliance complexity across
- **Focus on financial entities' ability to withstand, respond to, and recover** from all types of ICT-related disruptions and threats
- Consistent reporting of major ICT-related incidents with aim **to facilitate financial sector's response**
- **Enhancing ICT third-party risk management**, through contractual requirements and **oversight of critical ICT TPPs** by the ESAs
- **Enhancing testing and preparedness**, including regular advanced testing/TLPT for certain entities
- Increasing supervisors' capabilities and awareness of ICT risks and related incidents faced by financial entities
- Encouraged sharing of threat intelligence to raise sector-wide awareness

Digital Operational Resilience Act (3)

Scope and interaction with existing legislation/regulation

- ***Scope:*** A wide range of financial entities (21 different types), as well as ICT third-party providers (*refer to the annex*)
- DORA framework consists of a **regulation** (including supplementary technical standards and guidelines - *refer to the annex*) and a **directive** stipulating the changes to sectoral directives to enable coexistence
- ***ESAs' tasks:*** Policy implementation, Oversight of the critical ICT third-party providers (CTPPs) and IT implementation
- ***Proportionality:*** Overarching principle on the application of DORA requirements (Art.4), along with topic-specific proportionate approaches

- ***Interaction with other EU legislation***: (i) DORA constitutes **lex specialis** to horizontal NIS 2 Directive and (ii) **PSD2 incident reporting requirements ceased to apply to payment service providers** that fall under DORA
- ***Interaction with sectorial guidance***: (i) The scope of the EBA Guidelines on ICT and security risk management has been narrowed down and (ii) the EBA Guidelines on outsourcing arrangements are currently under revision due to DORA

Digital Operational Resilience Act (4)

Key pillars

DORA

ICT risk management

- Harmonised **ICT risk management** requirements

ICT-related incidents

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

Digital operational resilience testing

- **Testing programme** and coordinated **advanced testing** (with mutual recognition) for certain FEs

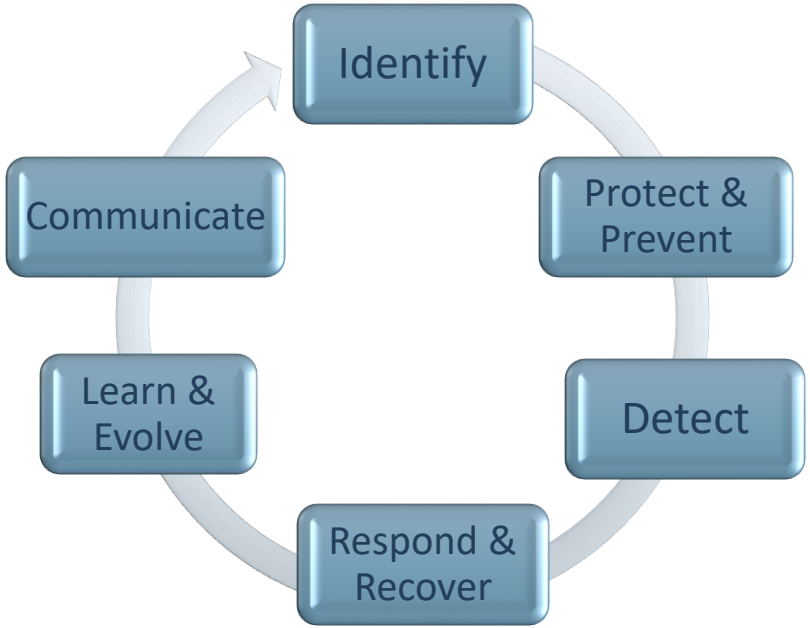
ICT third-party risk management

- Monitoring ICT third **party risks, key provisions**
- Establishing an **oversight framework for critical ICT TPPs**

Information sharing

- Exchange of information and intelligence on cyber threats

ICT risk management
Overview (Art.5-16)



ICT Governance and organisation

- **Overarching principle**: Ultimate responsibility of the management body in managing ICT risk, including continuous engagement in the control of the monitoring of the ICT risk management.

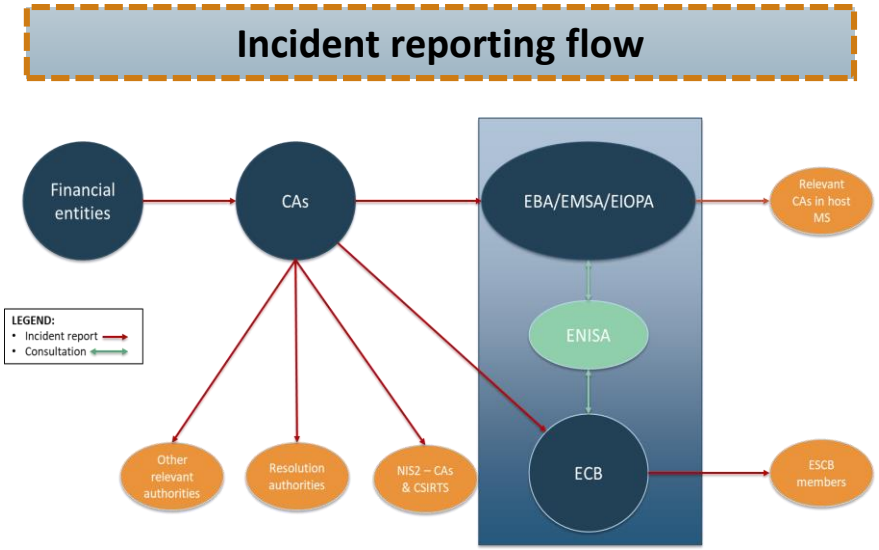
ICT Risk Management requirements

- A sound, comprehensive and well-documented **ICT risk management framework** needs to be in place
- This includes a **digital operational resilience strategy** (along with risk tolerance limit for ICT risk, information security objectives, etc.)

Simplified ICT risk management framework for small/exempted financial entities (small and non-interconnected investment firms, payment institutions exempted from PSD2, institutions exempted from CRD, e-money institutions exempted from e-money Directive)

ICT-related incident management, classification and reporting
Overview (Art.17-23)

- **ICT-related incident management process** to detect, manage, and notify incidents. This includes consistent monitoring, recording, handling, follow-up and proper communication.
- **Classification of ICT-related incidents** (and security and operational payment-related incidents) and significant cyber threats.
- **Reporting of major ICT-related incidents to CAs** and on voluntary basis significant cyber threats. Three types of reports for each incident: (1) Initial notification (early warning), (2) Intermediate report (status update) and (3) Final report (root cause identified).
- Classification thresholds, reporting timelines, content of the incident reporting, forms, templates and procedures are set out in RTSs and ITS



Digital operational resilience testing
Overview (Art.24-27)

Establish, maintain and review a DOR testing programme (integral part of the ICT RMF)

- Apply proportionality and risk-based approach
- Tests by independent parties
- Establish procedures, policies and internal validation methodologies to remedy and fully address issues revealed
- Conduct tests on all ICT systems/applications supporting C&I functions at least yearly

All financial entities (other than microenterprises*)

Assessment of basic requirements (e.g. vulnerability assessments and scans, network security assessments, gap analyses, questionnaires, scenario-based tests, penetration testing)

All financial entities (other than microenterprises*)

Perform advanced testing (TLPT) at least every 3 years

Large, systemic and ICT-mature financial entities

- Conclusions from relevant testing programme will trigger **review of relevant components of the ICT RMF.**
- Lessons derived from TLPT to be duly incorporated on a continuous basis into the ICT risk assessment process.

** Microenterprises subject to a more flexible testing regime*

Managing of ICT third-party risk
Overview (Art.28-30)

- Integral part of ICT risk management framework. If contractual arrangements are in place for the use of ICT services to run business operations, **financial entities shall remain fully responsible for compliance with DORA and applicable law**.
- Regular review of **ICT third-party risk strategy,** including a policy on the use of ICT services supporting C&I functions
- Maintain and update a **register of information** in relation to all contractual arrangements on the use of ICT services provided by ICT TPPs. To be made available to the competent authority, upon request. Competent authority shall be informed about any planned contractual arrangement on the use of ICT services supporting C&I functions.
- Need to consider several aspects (e.g. C&I functions, identification and assessment of all relevant risks, due diligence on prospective ICT TPPs, conflicts of interest, etc.) *before* entering a contractual arrangement on the use of ICT services.
- DORA sets **minimum elements to be included in contractual arrangements** on the use of ICT services. FEs may enter into a contractual arrangement only with ICT TPPs that comply with appropriate information security standards.
- **Exit strategies in place** for ICT services supporting C&I functions.

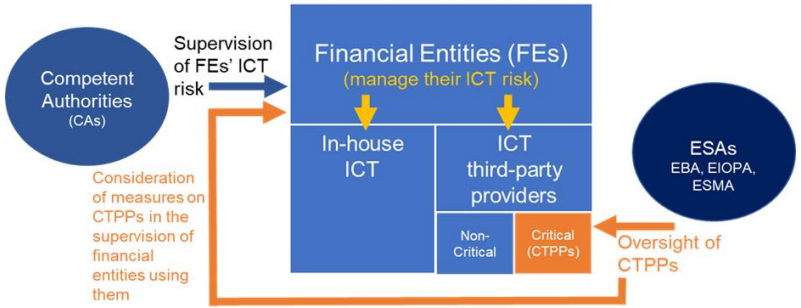
Managing of ICT third-party risk

Overview of oversight framework (Art.31-44)

- The **EU oversight framework on the critical ICT third-party service providers (CTPPs)** is established as part of the DORA ICT third-party risk management and it's entrusted to the three ESAs (EBA, EIOPA, ESMA) with the objectives (i) to assess whether CTPPs manage the ICT risks which may pose to financial entities and (ii) to allow for a continuous monitoring of the CTPPs' activities

- The oversight framework **complements** the existing supervision of financial entities in relation to the management of ICT third-party risk.

- Oversight activities to provide complementary insight and support to the supervisory work of the competent authorities.



Useful resources

- **EBA** – DORA: https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act
- **EIOPA** – DORA: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
- **ESMA** – DORA: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
- **European Commission** – DORA implementing and delegated acts: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en

In case you are interested to join the ESAs DORA team: https://www.eba.europa.eu/about-us/careers/vacancies

Thank you!

Annex

Annex

List of FEs within the scope of DORA

- credit institutions,
- payment institutions,
- electronic money institutions,
- account information service providers,
- investment firms,
- crypto-asset service providers and issuers of asset-referenced tokens;
- central securities depositories,
- central counterparties,
- trading venues,
- trade repositories,
- managers of alternative investment funds,
- management companies,
- data reporting service providers,
- insurance and reinsurance undertakings,
- insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries,
- institutions for occupational retirement pensions,
- credit rating agencies,
- securitisation repositories,
- administrators of critical benchmarks,
- crowdfunding service providers.

Annex
Supplementary technical standards and guidelines

ICT risk framework (Chapter II)

- RTS on ICT risk management framework (Art.15)
- RTS on simplified ICT 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 on specifying 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)

ICT third-party risk management (Chapter V.I)

- ITS on 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 (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)

Floor 24-27, Tour Europlaza
20 Avenue André Prothin
92400 Courbevoie, France

Tel: +33 1 86 52 70 00
E-mail: info@eba.europa.eu

https://eba.europa.eu/