



The EU's Digital Operational Resilience Act

SECURITY MATTERS FORUMS

Meeting you today



Jess Tasellari
Deloitte

Focus areas: Cyber Strategy, Governance and Controls. Regulatory engagement.



Matteo Orta
Deloitte

Focus areas: Regulatory strategy in operational resilience, digital markets and innovation regulation.

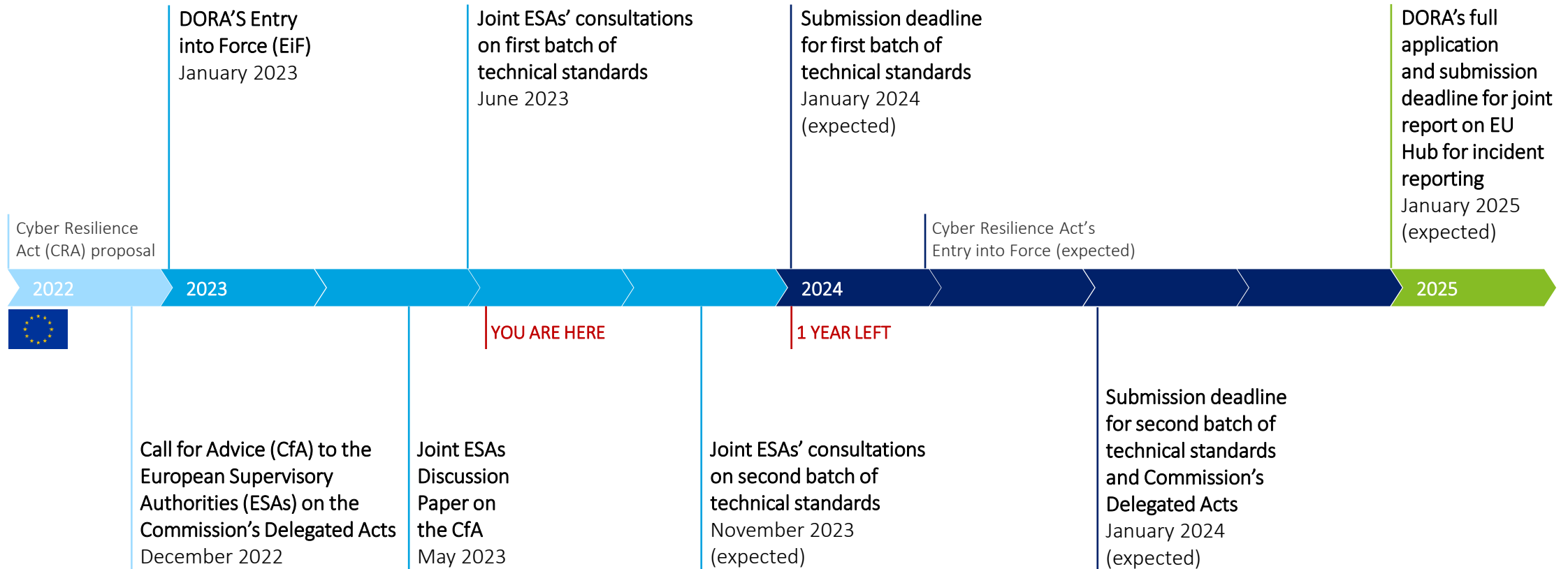
Agenda

1. Timeline
2. Five key pillars
3. Critical Third Party Oversight at a glance
4. Secondary legislation

The Digital Operational Resilience Act

Implementation Timeline

The DORA was published in the EU's Official Journal on 27th December 2022 and entered into force on 16th January 2023. A 24-month implementation period will precede full application in 2025.








● Negotiation Period
 ● Implementation Period (1st year)
 ● Implementation Period (2nd year)
 ● Full Application

The Digital Operational Resilience Act

Five key pillars

The DORA introduces a unified regulatory and supervisory rulebook for ICT operational resilience in the financial sector, pushing FS firms to make substantial investments to improve their resilience to digital and cyber risk disruptions.

		Objectives	Key requirements and implications
Four pillars for firms	 ICT risk management	Creating an ICT risk management framework around a set of key principles and requirements	<ul style="list-style-type: none"> ▪ Closely aligned to existing Guidelines (e.g. EBA ICT Risk Guidelines) but binding. ▪ Firms to set an internal framework for managing ICT risk and to focus on “Critical or Important Functions”. ▪ Mandatory Business Impact Analysis to be carried out based on “severe business disruptions”. ▪ Board/top management to hold ultimate accountability.
	 Incident reporting	Harmonising ICT incident classification and reporting	<ul style="list-style-type: none"> ▪ Harmonises multiple incident reporting rules into a single classification and reporting standard that mandates firms to carefully collect, manage and disseminate incident data. ▪ Obligation to classify cyberthreats and notify customers of exposure to “significant” cyber threats. ▪ Mandate for EU supervisors to investigate the potential for a single EU reporting Hub.
	 Digital operational resilience testing	Setting EU-wide standards for digital operational resilience testing (incl. threat-led penetration testing)	<ul style="list-style-type: none"> ▪ EU-wide requirement for resilience testing, including duty to test all critical functions at least annually and “fully address” any vulnerabilities identified. ▪ Creates a binding “advanced testing” requirement for larger firms (TLPT/TIBER/CBEST testing). ▪ Requires that Critical Third Parties be involved in some advanced testing.
	 ICT third-party risk	Harmonising minimum contractual elements of the relationship with ICT third parties	<ul style="list-style-type: none"> ▪ Closely aligned with existing Guidelines from ESAs but binding. ▪ Firms to adopt a proactive stance in ICT TPRM (e.g., mandatory contractual terms for outsourcing, requirement to assess concentration risks when outsourcing affects CIFs, etc.) ▪ Optional “Holistic Multi-Vendor Strategy”.
Pillar for ESAs	 Critical Third-Party oversight	Creating a direct oversight framework for critical third-party providers	<ul style="list-style-type: none"> ▪ Establishes the world’s first regime for allowing FS authorities to oversee and direct Critical Third-Party Providers (CTPs). ▪ Designated CTPs to demonstrate their resilience to the ESAs, which will be able to issue recommendations on improving resilience, and impose fines, etc.

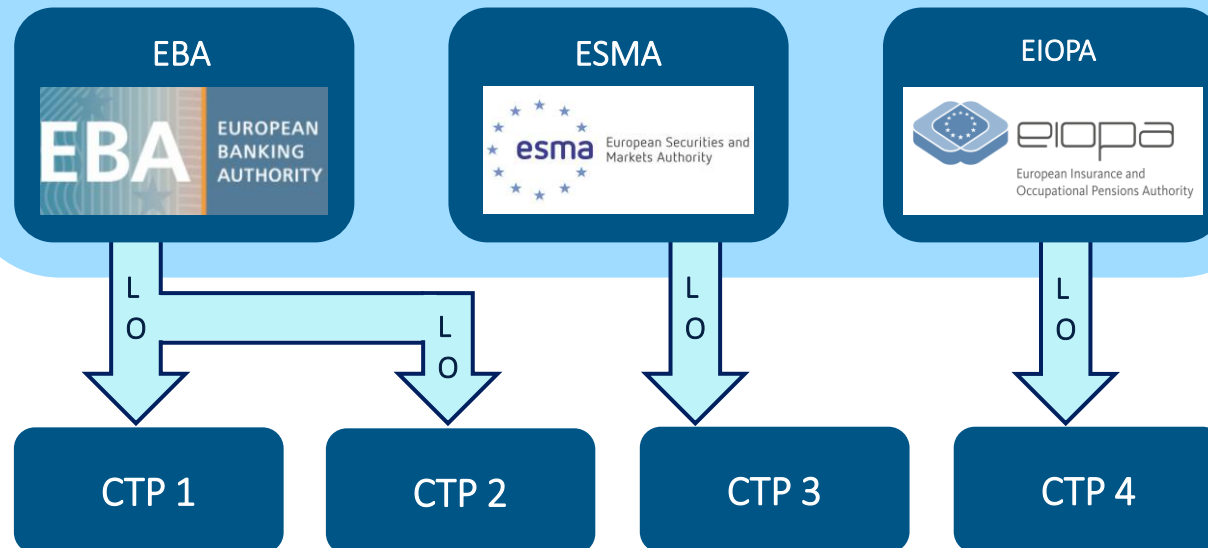
The Digital Operational Resilience Act

CTP oversight

The DORA establishes the world's first regime for allowing FS authorities to oversee and direct Critical Third-Party Providers (CTPs). Designated CTPs will have to demonstrate their resilience to the ESAs, which will be able to issue recommendations on improving resilience, and impose fines, etc.

JOINT OVERSIGHT FORUM

- Composed of ESAs' Chairpersons and Executive Directors, plus one representative from each EU member state's own National Competent Authority.
- Recommends designation of certain TPs as 'critical' and appoints one ESA as Lead Overseer (LO) of for each CTP.
- Coordinates oversight, keeps list of CTPs, and carries out yearly assessments.



CTP DESIGNATION CRITERIA

ESAs will designate certain third-party providers as 'critical' on recommendation of the JOF, based on the following criteria:

- Systemic impact in case of disruption of the TP.
- Systemic importance of the FS firms relying on that TP.
- Number of CIFs serviced by the TP.
- Degree of substitutability of the TP.

TPs are allowed to submit voluntary designation requests too.

LEVEL 2 LEGISLATION

July 2024

- Commission's DA to further specify CTP designation criteria and oversight fees.
- RTS to further specify details on CTP oversight (e.g., coordination between the ESAs, assessment criteria, etc.).

The Digital Operational Resilience Act

Secondary legislation

The DORA delegates a large portion of relevant technical detail to Level 2 initiatives to be drafted by the European Supervisory Authorities. This will, in many cases, mean that firms will have to wait even longer for clarity on the practical aspects of the DORA's new rules.

ESAs' FIRST BATCH OF TECHNICAL STANDARDS

- Regulatory technical standards (RTS) on harmonisation of ICT risk management tools, methods, and processes.
- RTS on simplified version of the risk management framework for small firms.
- RTS on classification of ICT-related incidents and significant cyber threats.
- Implementing technical standards (ITS) on the Register of Information on third-party providers (TPs).
- RTS on TP risk management and contractual measures for TPs supporting critical or important functions.

ESAs' SECOND BATCH OF TECHNICAL STANDARDS

- RTS on advanced testing methodologies, scope and criteria for selecting testers.
- RTS on TPs' subcontracting of critical or important functions.
- RTS on forms, templates and procedures to report major ICT-related incidents and significant cyber threats.
- Guidelines on estimation of aggregated losses caused by ICT-related incidents.
- Guidelines on supervisory cooperation within the Joint Oversight Network
- RTS on harmonisation of conditions for oversight activities.

COMMISSION'S DELEGATED ACTS

- Delegated Act on designation criteria for critical third-party providers (CTPs).
- Delegated act on Lead Overseer-related supervision fees for CTPs.

ESAs' JOINT REPORT

- Report on the feasibility of a single EU Hub for ICT-related incident reporting.



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.