Digital Operational Resilience Act (DORA)

How DORA will impact the financial services industry

Webinar

05/10/2023

arendt.com

CONFIDENTIALITY REMINDER
This document is confidential and is intended solely for its recipient.
Do not distribute outside your organisation.

Digital Operational Resilience Act (DORA)

Your contacts/speakers

Bénédicte d'Allard

Senior Manager
Regulatory Consulting

Pierre-Michaël de Waersegger

Partner
Insurance & Reinsurance Law

Marc Mouton

Partner
Banking & Financial Services

Henning Schwabe

Partner
Investment Management

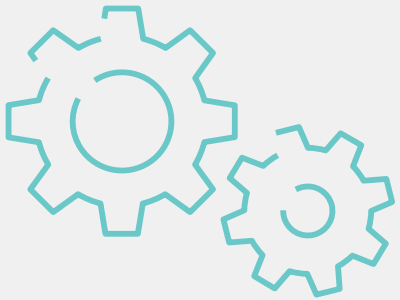
Astrid Wagner

Partner
IP, Communication & Technology

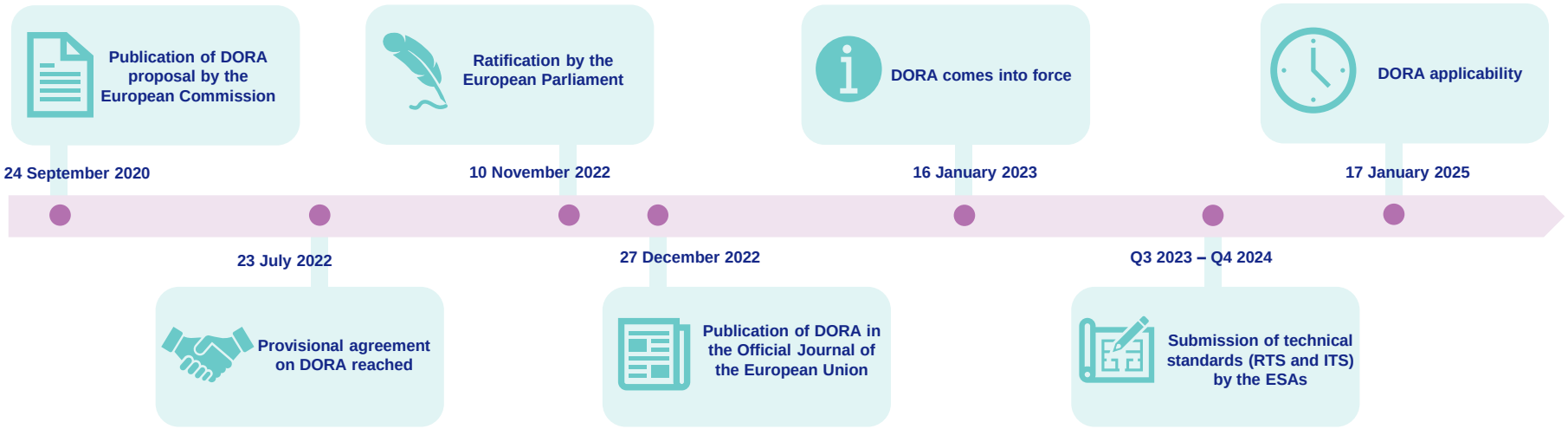
arendt.com

Background

- **Digital Finance Package** adopted on 24 September 2020 by the EU Commission
  - digital finance strategy
  - legislative proposals on crypto-assets (MiCA proposal) and digital resilience
- **Need to prevent and mitigate cyber threats**
  - Use of ICT and ever-increasing digitalization core to the activities of financial entities
  - Heavy dependency on third parties providing ICT services
  - Amplification of ICT risks through increased digitalisation and interconnectedness
  - Ever-increasing risks of cyber attacks
- **Interactions with NIS2 and GDPR**



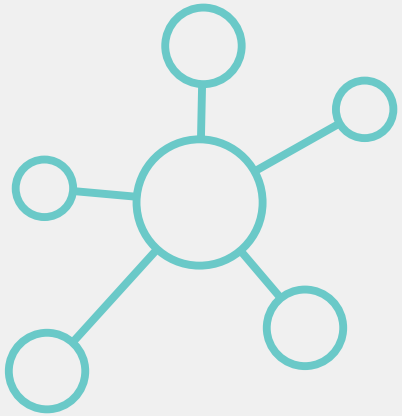
Implementation timeline



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 June 2024 (second batch) as highlighted below.

Policy mandates	Public consultation	Finalised
Call for advice on criticality criteria and fees	26 May – 23 Jun ‘23	30 Sept ’23
1st batch of mandates (Art.15, 16(3), 18(3), 28(9) and 28(10) DORA)	16 Jun – 11 Sep ’23	17 Jan ‘24
2nd batch of mandates (Art.11(11), 20a, 20b, 26(11), 30(5), 32(7) and 41 DORA)	Nov/Dec’23 - tbc	17 Jul ‘24

In scope entities



- **Financial entities**
  - Banking sector
  - Insurance sector
  - Asset management sector
  - ICT third-party service providers

Five pillars of resilience

DORA creates a **regulatory framework on digital operational resilience whereby all EU financial entities are required to ensure they can withstand, respond to and recover from all types of ICT-related disruptions and threats**.

DORA

First pillar
ICT risk management

- ICT responsibilities of management body
- Sound, comprehensive and well-documented ICT risk management framework (“RMF”), incl. digital operational resilience strategy
- ICT resilience strategies, policies, procedures
- ICT protocols & tools protecting information & ICT assets

Second pillar
ICT-related incident management, classification and reporting

- Detection, classification, monitoring of ICT incidents
- Reporting of major ICT-related incidents
- Recording and notification of cyber threats affecting customers or counterparties

Third pillar
Digital operational resilience testing

- Risk-based approach
- Annual security and resilience tests on critical ICT systems and applications
- Procedures and policies to prioritize, classify and remedy issues revealed
- Addressing identified vulnerabilities

Fourth pillar
Managing of ICT third–party risk

- Monitoring of ICT third-party service providers
- Identification of critical or important functions
- Register of third-party contractual relationships
- Key contractual provisions
- Exit strategies for critical or important functions

Fifth pillar
Information-sharing arrangements

- Voluntary exchange of cyber threat information and intelligence among financial entities

Main focus

Governance Extensive documentation Reliable & adequate tools	Internal & external watch Audit trail & classification Reporting	Documentation Follow-up feeding updates of ICT Risk management framework	Governance Classification and documentation Contracts	Optional

Impact on the financial entities

Is DORA a game changer?

Bill of law n° 8291

Powers of the CSSF and the CAA

Potential fines and other administrative measures

DORA

List of RTS/ITS

Two main submission deadlines for the sets of policy products : 17 January 2024 & 17 June 2024

ICT risk framework

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

ICT related incident management classification and reporting

- **RTS on criteria for the classification of ICT related incidents (Art.18.3)**
- *To come* : RTS to specify the reporting of major ICT-related incidents (Art.20.a)
- *To come* : ITS to establish the reporting details for major ICT related incidents (Art.20.b)
- *To come* : 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

- *To come* : RTS to specify threat led penetration testing (Art.26.1)

Oversight framework

- *To come* : Guidelines on cooperation ESAs- CAs (Competent Authorities) regarding DORA oversight (Art. 32.7)
- *To come* : RTS on harmonisation of oversight conditions (Art.41)

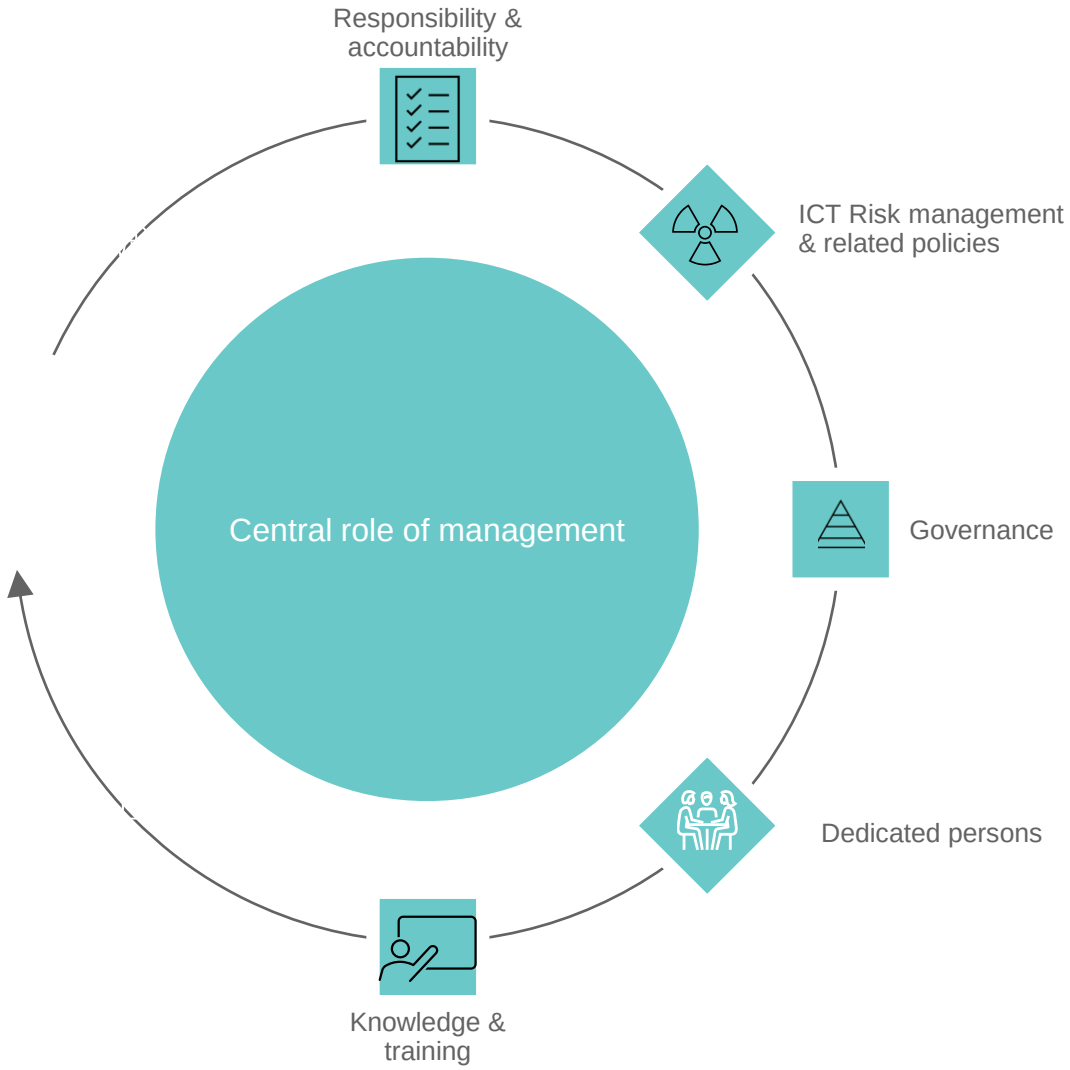
Third-party risk management

- **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)**
- *To come* : RTS to specify the elements to determine and assess when sub-contracting ICT services supporting a critical or important function (Art.30.5)

+ ESA delivered on 30 Sept 2023 pieces of advice on criticality criteria (Art.31.8) and fees (Art.43.2)

Bold = policy mandates with deadline 17 January 2024 (first batch)

Role & liabilities of the management body

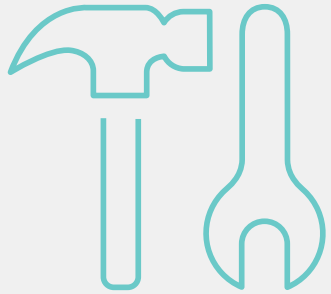


Best approach for DORA implementation and how Arendt can assist

Start early

Focus on an initial thorough strategic analysis (e.g. critical functions & assets)

Keep in mind DORA's motto - consistency & alignment of/with the ICT risk management framework



- **Gap analysis** between your company's current situation in terms of ICT governance, ICT risk management, and compliance compared to DORA requirements.
- **Trainings** to staff members and board members
- **Drafting or review of relevant documentation** : digital operational resilience strategy, ICT policies, procedures and inventories
- **Drafting or review of agreements** with ICT third-party providers
- **Design/ review of process** (e.g. incident management)
- **Project management** support
- **ICT risk analysis**

Your contacts/speakers

Bénédicte d'Allard

T (352) 26 09 10 77 31
benedicte.dallard@arendt.com

Pierre-Michaël de Waersegger

T (352) 40 78 78 258
pierre-michael.dewaersegger@arendt.com

Marc Mouton

T (352) 40 78 78 336
marc.mouton@arendt.com

Henning Schwabe

T (352) 40 78 78 525
henning.schwabe@arendt.com

Astrid Wagner

T (352) 40 78 78 698
astrid.wagner@arendt.com

Thank you!