iapf representing pension savers

Digital Operational Resilience Act

Trustee Awareness Session

Agenda

What is DORA?

What is DORA?

The Digital Operational Resilience Act (DORA) is a new European regulation that defines detailed and comprehensive regulations for digital operational resilience at EU level.

DORA will apply to 22,000 regulated organisations* in the EU and approximately 16,000 third parties globally to ensure convergence and **harmonization** of security and resilience practices **across the EU.**

DORA entered into force on **January 16, 2023.** Subsequent specifications in form of RTS (Regulatory Technical Standard) and ITS (Implementation Technical Standard) are planned. There is a transition period of 24 months in total for implementation.

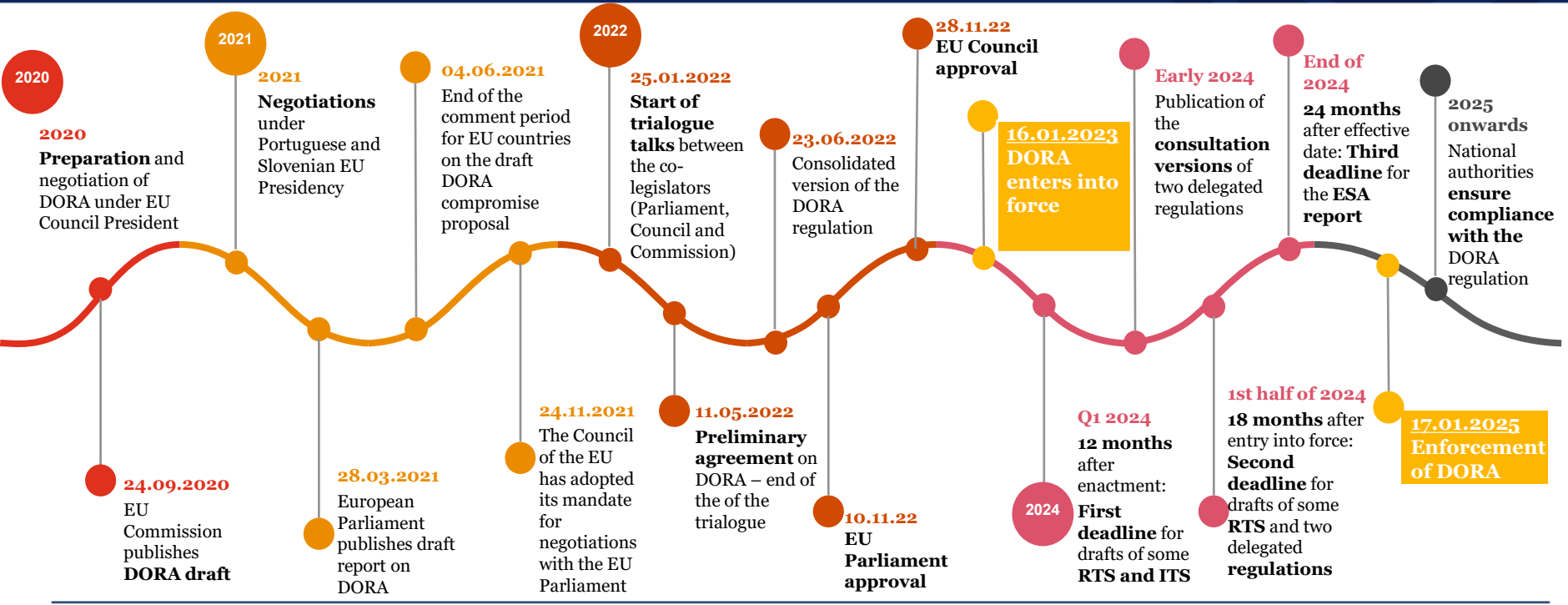
DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats."

- Council of EU

Purpose

- Ensure that financial entities and third-party providers (TPP), respond to and recover from all types of ICT-related disruptions in a timely and appropriate manner
- To mitigate risk posed by growing vulnerabilities, due to increasing interconnectivity of the financial sector.
- To address the shift in risk profile as a result of the increase of financial services digital adoption.
- To acknowledge and address the third party reliance underpinning the stability of the financial sector.
- To adopt a single, consistent supervisory approach to operational resilience across the single market.
- Harmonise ICT risk management rules across financial services sectors, based on existing guidelines.
- Harmonising ICT incident classification and reporting
- Empower financial supervisory authorities to monitor and audit financial entities and their third-party ICT providers more closely

Where did DORA come from?



RTS Timeline

The first consultation phase has started and the two-year implementation period is already underway

Entry into force

DORA entered into force on 16. Jan. 2023

Public consultation

First public consultation on 5 RTS / ITS

Public consultation

Second public consultation on 6 RTS / ITS

Publication of all RTS / ITS

By September of 2024 all specifications should be published

Enforcement

iapf representing pension savers

DORA key areas/pillars

As the operational risks could exist at many levels across an organization, even outside a company such as third parties, the DORA directives covers 5 key areas/pillars that are relevant for the reporting entities. See Appendix 1 for further information.

ICT risk management

- The **ICT risk management framework** must be detailed and aligned with the corporate strategy and objectives
- A **strategy for digital resilience** must be defined
- **Enhance first line of defense capabilities**, from threat detection to response, recovery, and communications, with emphasis on - but not limited to:
  - Threat scenario modeling
  - Cyber protection and prevention
  - Business continuity and disaster recovery Communication (e.g. with customers)

Incident reporting

- **Reporting** of ICT-related incidents (and significant cyber threats)
- Submission of **initial, interim, and final reports** on serious ICT-related incidents (and significant cyber threats)
- Conducting a **root cause analysis** after ICT-related incidents
- Identification and **reporting of required improvements**

ICT third-party risk

- Integration into ICT risk management framework
- Essential **contractual requirements**
- Keeping an information register on all services **provided by ICT third parties**
- **Reporting on changes** in the use of critical ICT services
- Assessment of **ICT concentration risk** and **sub-outsourcing**
- Restricted use of third-party ICT providers **in third countries**

Digital operational resilience testing

- **Annual testing** of all critical ICT systems
- Advanced **threat-led penetration testing** every 3 years
- **Involvement of ICT third-party** providers

Information sharing

- **Sharing cyber threat intelligence** and insight to improve digital operational resilience
- **Agreements** on the exchange of information (incl. conditions for participation)
- Implementation of **mechanisms to review and take action** on the information shared by the authorities

- Ultimate aim is to have a **digitally resilient EU marketplace** that protects EU consumers of financial services products.
- Local regulatory **oversight and penalties** for non compliance from Jan 2025. Ongoing compliance will challenge organisations for years to come.

RTS and ITS Timeline

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) DL: 29 Sept 2023**
- Guidelines on cooperation ESAs – CAs (Competent Authorities) regarding DORA oversight (Art. 32.7)
- RTS on harmonisation of oversight conditions (Art. 41)

Legend

Bold Pink: RTS's that have been circulated to date

- **Public Consultation** 16 Jun 23 - 11 Sep 23.
- **Finalised** 17 Jan 2024

Bold Grey: RTS's released in December 2023

- **Public consultation**: Until March 8th 2024
- **To be finalised**: 17 July 2024

iapf representing pension savers

DORA In scope entities

DORA applies to a wide range of entities within the financial services sector under Article 2 of the Act

- credit institutions
- payment institutions
- account information service providers
- electronic money institutions
- investment firms
- central securities depositories
- **institutions for occupational retirement provision**
- central counterparties
- credit rating agencies
- administrators of critical benchmarks
- crowdfunding service providers
- securitisation repositories
- ICT third-party service providers
- 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
- crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets,and issuers of asset-referenced tokens

DORA out of scope entities

The following entities are deemed out of scope for DORA	
a) Alternative investment fund managers	Managing one or more alternative investment funds with real assets worth less than EUR 100 million or less than EUR 500 million if they are not leveraged.
b) (Re)Insurance undertakings	Taking up direct insurance activities or reinsurance activities and not exceeding annual gross premiums of EUR 5 million and technical provisions of EUR 25 million.
c) institutions for occupational retirement provision which operate pension schemes	…which together do not have more than 15 members in total;
d) certain natural and legal persons	For example, persons whose investment services consist solely of the administration of employee benefit plans are exempt.
e) (Re)Insurance undertakings who are microenterprises or small or medium-sized enterprises	No more than 250 people may be employed, annual sales may not exceed EUR 50 million and/or the annual balance sheet total may not exceed EUR 43 million.
f) Postal giro offices	Post giro offices, formerly post office check offices, which are now part of Deutsche Postbank AG.

A typical DORA journey...

Governance Structure

Determine the **key stakeholders** to be involved in your DORA journey noting the **cross functional approach** required.Identify an overall project sponsor, steerco etc and establish **project governance.**

Awareness & training

Providing **training to your Board** or Management team on the **DORA requirements and roles and responsibilities** of the various stakeholders

Identification & mapping of CIBF's

Identification of "Critical or Important functions(CIF's)

- Identify and map your **"Critical or Important functions"** to your IT landscape for your organisation including where these extend to your **third party providers and beyond.**

Completion of Register of Information

DORA provides a **template f**or completion which requires organisations to document **105 data points on each of their third party providers**. Both those supporting **CIBF's** and those that are denoted under Annex 3 as one of the **19 categories of ICT providers.**

Gap Assessment

DORA "Gap" Assessment

- Conduct, through a series of **workshops**, a perform a gap assessment against the the defined DORA requirements in each DORA pillar.

Implementation

Prepare a **roadmap to compliance** for the gaps identified and **implement those gaps** in relation to each of the DORA pillars

Update and agree third party contracts

DORA requires all **third party contracts** to be **reviewed and updated** to include the **requirements of DORA.**

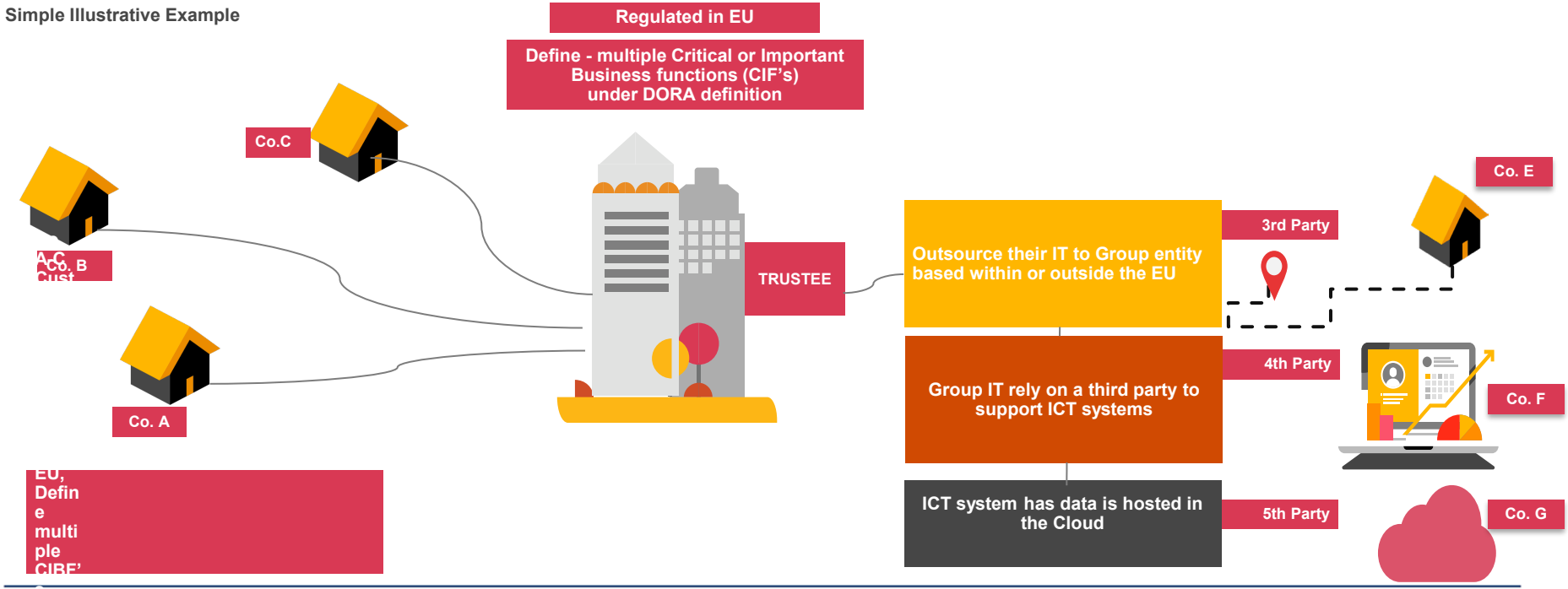
Define and report on the requirements of DORA to your Board

The **Board has ultimate responsibility** for DORA and therefore they will be required to **oversee and approve key** aspects of the DORA requirements.

iapf representing pension savers

Value chain - simplifying complexity is difficult

Simple Illustrative Example



iapf representing pension savers

The Trustee & DORA

Regulatory Oversight

Oversight

For Pension Schemes, The Pensions Authority will perform regulatory oversight over trustees Compliance with the DORA regulation

Responsibility for DORA is the ultimate responsibility of the management body. This is interpreted to be the Trustees of the Board of the institutions for occupational retirement provision

An tÚdarás Pinsean
The Pensions Authority

iapf representing pension savers

Responsibilities of the Trustee

Responsibilities of the Management Body (Article 5)

Bear the **ultimate responsibility** for managing the financial entity's ICT risk

Implement **policies** to ensure high standards of **availability, authenticity, integrity and confidentiality, of data**

Set **clear roles and responsibilities** for all ICT-related functions and establish appropriate governance arrangements to ensure **effective and timely communication, cooperation** and coordination among those functions;

Bear the overall responsibility **for setting and approving the digital operational resilience strategy**, including the determination of the appropriate risk tolerance level of ICT risk of the financial entity.

ICT Third-Party Service Providers:

Approve and periodically review the financial entity's policy on arrangements regarding the **use of ICT services provided by ICT third-party service providers;** (i) put in place, at corporate level, reporting channels enabling it to be duly informed of the following:

- **arrangements concluded** with ICT third-party service providers on the **use of ICT services,**
- any **relevant planned material changes** regarding the ICT third-party service providers,
- the **potential impact of such changes on the critical or important functions** subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.

Approve and periodically review the financial entity's ICT internal audit plans, ICT audits and material modifications to them;

Allocate and periodically review the appropriate budget to fulfil the financial entity's **digital operational resilience need**s in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training

Approve, oversee and periodically review the implementation of the financial entity's **ICT business continuity policy and ICT response and recovery plans,**

Actively **keep up to date with sufficient knowledge** and **skills** to **understand and assess ICT risk** and its impact on the operations of the financial entity, including by following **specific training on a regular basis,** commensurate to the ICT risk being managed.

iapf representing pension savers

Third Party Contractual Arrangements

Contractual Provisions

DORA prescribes minimum **contractual arrangements** which **FE's need to incorporate into the current contracts** with their TPP. Therefore the FEs will reach out to each TPP to update or respectively supplement their current contracts in place.

Relevant **clauses** of the contractual arrangements need to be **replicated in the subcontract arrangements** if the service supports a CIBF*

Key contractual arrangements with TPP must contain:

- Clear and comprehensive **description of the functions and services** of the TPP as well as special provisions for subcontracting
- **Location** where activities are performed and data is processed/stored
- **Provisions** for the **confidentiality, integrity, availability**, and security of personal data
- Requirements for **ensuring access to personal and non-personal data** (including in the event of insolvency)
- Descriptions of the **service level**
- **Provision of assistance in case of an incident** (free of charge; ex ante)
- **Obligation** to **cooperate with supervisory authorities**
- **Termination rights** (with definition of an appropriate notice period)
- Conditions for the **participation** of the TPP in the FE's IT **security awareness programmes**

If the service supports a FE CIBF* further contractual provisions are required:

- Clear and comprehensive **description of the functions** and services provided by the TPP, including service levels, **qualitative and quantitative performance objectives**, including updates and revisions.
- **Reporting and information obligations (including incidents)** for the TPP in the event of changes that pose potential risks to the financial institution, impact on the services provided, or agreed service levels.
- **Obligation** for the TPP **implement and test plans for business continuity and emergency recovery**, and to have in place **ICT security measures, tools and policies**
- Commitment of the TPP to **participate in the Digital Operational Resilience Test Program**, including **TLPT**.
- Right to **monitor the performance** of the TPP through access, inspection, and **audit**.
- **Exit strategies** (with definition of an appropriate transition period)

Questions Trustees should ask to TPP's

Responsibilities of the Management Body (Article 5)

Initial Engagement queries?	Third party queries	Contracting queries	Reporting
Do you have a DORA compliance programme in place to support us as third party provider to our CIBF's? Do you have a plan in place to provide us with the information to support us with compliance? What information do you require from us to commence this process? Where are you on this compliance journey? • Have you completed a mapping of your ICT systems supporting CIBF's in relation to the pension schemes you are supporting for our organisation? • Have you completed a gap assessment against the requirements of DORA? • Are you planning on being fully compliant before January 17th 2025?	Have you considered and mapped all of your sub contractors in relation to the processes you support on our behalf? In completing our "Register of Information" - can you provide us with all of our impacted third party providers and sub contracted providers or is there information you require from us in advance of providing such information?	We are required to update our existing contract with you to include the DORA contract requirements? Who do we engage with on this process? Who is responsible for applying the subcontracting requirements with your third parties which support our CIBF's?	What is the reporting structure for DORA implementation and oversight into the Trustees? How will we as the Trustees obtain sufficient oversight of DORA?

As an "institution for occupational retirement provision" we fall under the scope of DORA Article 2. We therefore have requirements under the Act to ensure we are compliant by 17th of January 2025.

Our Trustees bear the ultimate responsibility under DORA however, our "Critical or Important Business functions" rely on your organisation and therefore we understand you would be defined as our third party provider under the scope of DORA.

iapf representing pension savers

THANK YOU

iapf

representing pension savers