Preparing for the Digital Operational Resilience Act (DORA)

Legal update to the Irish Association of Pension Funds

EVERSHEDS SUTHERLAND

23 November 2023

Jane McKeever
Of Counsel | Pensions
Eversheds Sutherland LLP

Contents

- What is DORA and why is it required?
- Who does DORA apply to?
- Specific impact of DORA on pension schemes
- Regulatory Technical Standards and Implementing Technical Standards
- Who polices DORA/Role of the Pensions Authority
- Timeline

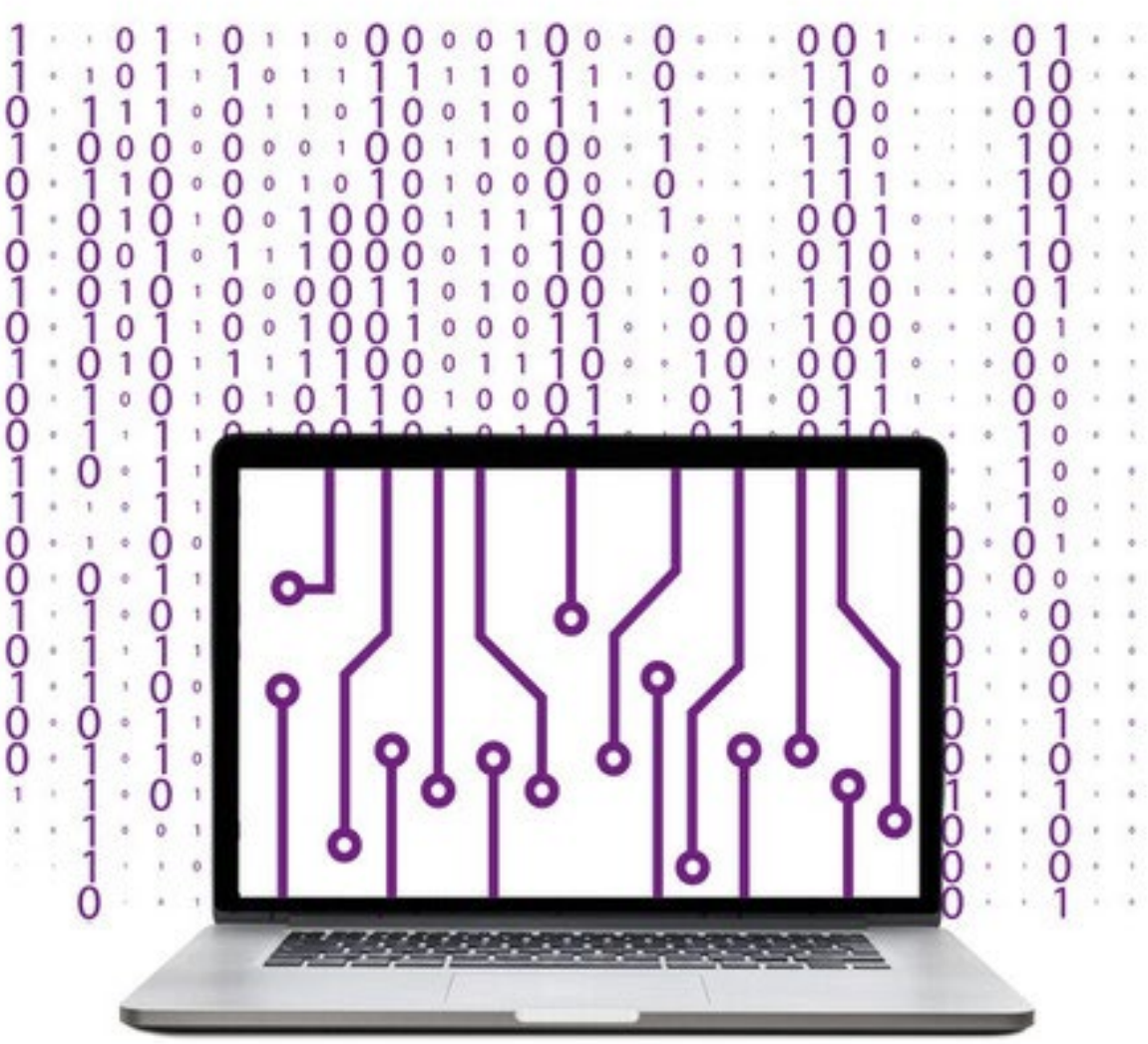
What is DORA?

The Digital Operational Resilience Act (DORA) – Regulation (EU) 2022/2554

- Regulation as opposed to Directive
  - Regulations are binding in their entirety on all EU countries as soon as they enter into force, without needing to be transposed into national law
  - Directives (eg the IORP II Directive) require EU countries to achieve a certain result but allow them flexibility regarding how to do so - EU countries must transpose Directives into national law
- Directly effective across the EU from 17 January 2025

Why is DORA required?

- Information Communication Technology (ICT) used to support every-day activities
  - ICT is any technological tool used to communicate information (eg, software applications and operating systems, web-based apps, member portals)
  - Used for example for payments, securities clearing and settlement activities, electronic trading, credit rating and claim management
- ICT incidents have the potential to jeopardise the stability of the entire financial system



Why is DORA required?

Increased interconnectedness means risk no longer limited geographically – global systems

Malicious actors becoming ever more sophisticated

Action required at an EU level to bolster resilience and avoid disruption to business and protect consumers

DORA consolidates and updates rules on ICT risk

- Introduces specific and prescriptive requirements that are homogenous across the EU
- Should strengthen resilience to ICT related incidents
- Also builds bank of information with respect to cyber incidents and threats

Who does DORA apply to?

DORA applies to financial institutions in the EU

Very broad scope - eg banks, investment firms, crypto-asset service providers and Institutions for Occupational Retirement Provision (IORPs) *(Article 2(1))*

Notably applies in part to third-party service providers that supply financial entities with ICT systems and services (eg, cloud service providers and data centres)

Certain entities excluded or treated differently

IORPs with less than 15 members excluded from application *(Article 2(3))*

IORPs with less than 100 members – "simplified" risk management framework *(Article 15)*

Accountability is established at management level – with trustees for pension schemes *(Article 5)*

Key obligations applicable to IORPs/pension schemes

5 key pillars to DORA

1

Risk Management *(Article 6 - 16)*

- Trustees expected to define appropriate risk management strategies, actively assist in executing them and stay current on their knowledge of ICT risk landscape
- Map ICT systems
  - Identify and classify critical assets and functions
  - Document dependencies between assets, systems, processes and providers
- Conduct continuous risk assessment on ICT systems, document and classify cyber threats
- Put appropriate cybersecurity protection measures in place; including policies and technical controls/solutions
- Establish business continuity and disaster recovery plans for cyber risk scenarios
- Document steps taken to mitigate identified risks

Key obligations applicable to IORPs/pension schemes

2

Incident Reporting (Articles 17 – 23)

- Trustees to establish systems for monitoring, managing, logging, classifying and reporting ICT-related incidents
- Significant ICT related breaches or incidents to be reported to the Pensions Authority (and potentially to affected members, counterparties and the public)
- Critical incidents also require intermediate report on progress towards resolving incident and final report analysing root causes of incident
- Cyber threats to be recorded
- System to be put in place to allow voluntary reporting of cyber threats

Key obligations applicable to IORPs/pension schemes

3

Digital operational resilience testing (Articles 24 – 27)

- Robust resilience testing on ICT security measures to be carried out at least annually
- Certain entities judged to play critical role in financial system to conduct "threat-led penetration testing" using live systems
  - Critical ICT providers to participate
- Approach intended to allow entities to detect and mitigate against vulnerabilities and breaches
- Results of tests and plans for addressing weaknesses to be reported to Pensions Authority

Key obligations applicable to IORPs/pension schemes

4

Third-party risk management

- Trustees will be expected to take an active role in managing ICT third-party risk
  - Risk assessments of such service providers to be carried out
  - ICT dependencies to be mapped
- DORA specifies multiple contractual terms to be included in contracts with ICT service providers including around
  - Exit strategies
  - Audits
  - Performance targets for accessibility, integrity and security
- Pensions Authority can suspend or terminate contracts that don’t comply
- Critical ICT third-party providers also subject to direct oversight from ESA Lead Overseers

Key obligations applicable to IORPs/pension schemes

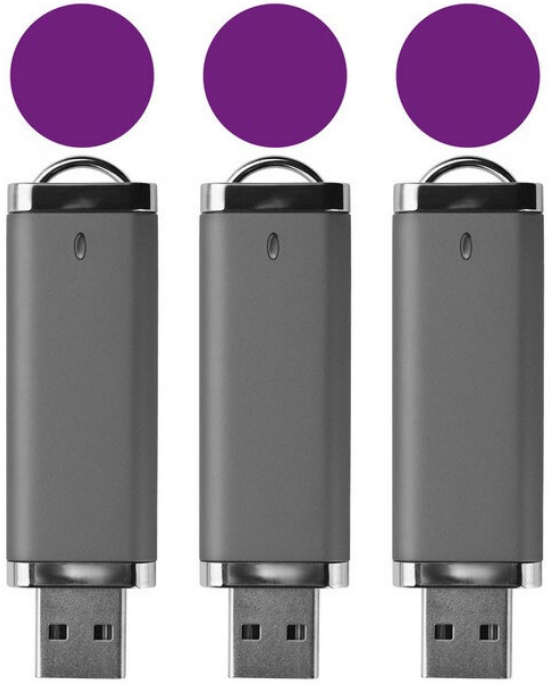
5

Intelligence sharing (Article 45)

- Processes to be established for learning from internal and external ICT-related incidents
- DORA paves the way for sharing of information and intelligence regarding cyber-threats
  - Trusted community of financial entities to facilitate this
  - To be implemented through information-sharing arrangements that protect the potentially sensitive nature of information shared
  - Competent authorities to be notified of participation in injunction sharing arrangements

Simplified regulation – Schemes with less than 100 members *(Article 16)*

- Certain smaller entities permitted to comply a "simplified" ICT risk management framework
- Still significant requirements including:
  - Put in place and maintain sound and documented ICT risk management framework aimed at quick, efficient and comprehensive management of ICT risk
  - Continuously monitor security and functioning of all ICT systems
  - Minimise ICT risk through use of sound, resilient and updated ICT systems, protocols and tools
  - Identify key dependencies on ICT third-party service providers
  - Put in place business continuity plans and response and recovery measures and test these plans and measures
  - Implement relevant operational conclusions resulting from tests



Proportionality principle

Article 4

- **Chapter II (risk management)** to be implemented by entities taking into account their size and overall risk profile and the nature, scale and complexity of services, activities and operations
- Application of **Chapter III (ICT related incident management and reporting), Chapter IV (Digital Operational Resilience Testing), Chapter V, Section I (Managing of third-party risk)** shall be proportionate to their size and overall risk profile and the nature, scale and complexity of services, activities and operations as specifically provided for in the relevant rules of those Chapters

ESAs and RTS/ITS

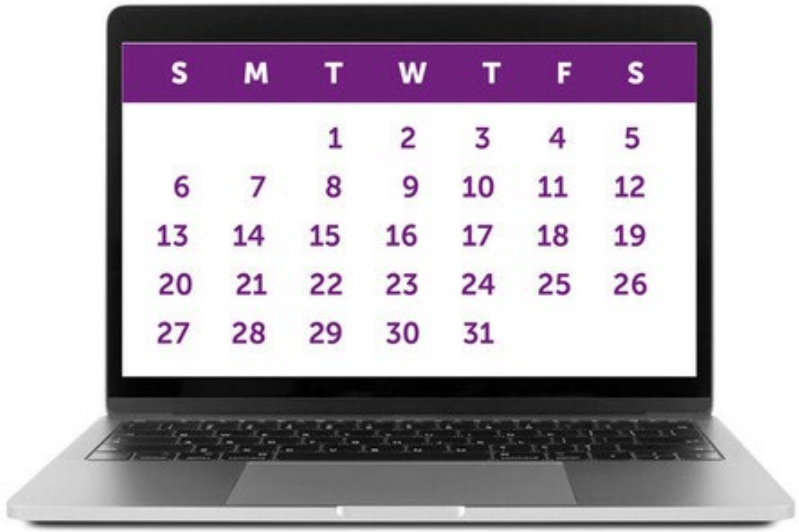
Under the Regulation, the European Banking Authority (**EBA**), European Insurance and Occupational IAPF(**EIOPA**) and European Securities and Markets Authority (**ESMA**) collectively are the European Supervisory Authorities ('**ESAs**')

The ESAs are obligated to draft regulatory technical standards (RTS) and implementing technical standards (ITS) to assist entities to understand their obligations

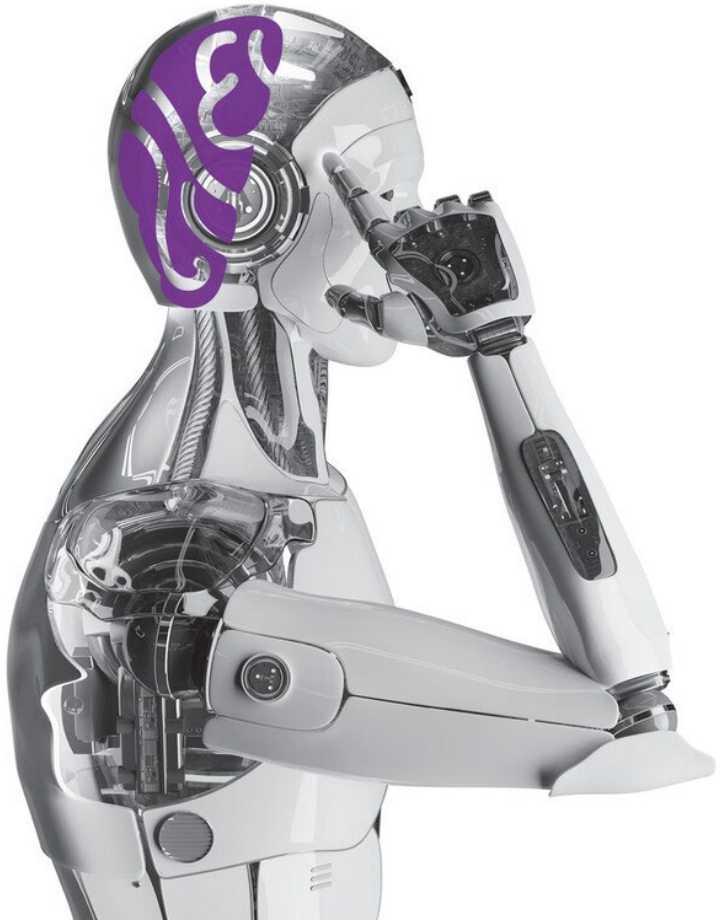
In-scope entities must abide by the technical standards

RTS/ITS

- First batch of RTS and ITS published for consultation on 19 June 2023
  - RTS on ICT risk management framework
  - RTS on simplified risk management framework
  - RTS on criteria for classification of ICT related incidents
  - ITS to establish the templates for the register of information in relation to contractual arrangements with ICT third-party service providers
  - RTS to specify the policy on contractual arrangements with ICT third party providers
- First batch to be submitted by 17 January 2024
- Second batch to be submitted by 17 June 2024



Who polices DORA?



- National competent authorities will take the role of compliance oversight and enforcement – Pensions Authority
- Broad enforcement powers
  - Accessing documents or data held in any form
  - On-site inspections
  - Competent authorities can request entities to take specific security measures and remediate vulnerabilities
- Member States to lay down appropriate administrative penalties and remedial measures for breaches
  - Minimum measures specified
  - Option of criminal penalties for certain breaches
- "Critical" third-party service providers to be directly supervised by "Lead Overseers" from ESAs

What can we expect from the Pensions Authority?

Article 46 confirms that, for IORPs, the competent authority is designated in accordance with Article 47 of Directive (EU) 2016/2341 (the IORP II Directive)

Recital 21

- To facilitate efficient supervision of IORPs that is proportionate and addresses need to reduce administrative burden on competent authorities, national supervision arrangements to take into account "*size and overall risk profile and the nature, scale and complexity of their services*"
- Focus primarily on need to address serious risks associated with the ICT risk management of a particular entity
- Competent authorities to maintain a "vigilant but proportionate approach" with respect to IORPs which outsource a significant part of their core business such as asset management, actuarial calculations, accounting and data management to service providers

Timeline

December 2022 DORA published

17 January 2024 First batch RTS and ITS to be submitted

17 June 2024 Second batch RTS and ITS to be submitted

17 January 2025 DORA comes into force across EU member states

EVERSHEDS SUTHERLAND

Contact: Jane McKeever

Of Counsel | Pensions

Eversheds Sutherland LLP

E: janemckeever@eversheds-Sutherland.ie