



Digital Operational Resilience: Are you ready?

Enabling innovation and competition for digital finance

February 2022

“Digital operational resilience means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality.”¹

Launched as part of the European Commission’s Digital Finance Package in September 2020, the Digital Operational Resilience Act (DORA) aims to improve the overall digital operational resilience of the financial sector. In November 2021, the Council of the European Union reached agreement and with European Parliament will now enter trilogue negotiations on the proposals.

The DORA Objectives

DORA will aim to harmonise existing legislation and supplement existing gaps with the introduction of new regulations to establish a unified digital framework whereby firms ensure they can adapt and endure all types of ICT-related disruptions and threats, in order to prevent and mitigate cyber threats. DORA sets out the following objectives:



Increase the collective digital resilience of the financial sector



Harmony across and access to ICT incident reporting information



Identify ICT vulnerabilities and analyse the efficacy of resilience measures against these vulnerabilities



Streamline the existing inconsistent regulatory approach across member states



Increase the contractual safeguards in the use of ICT services



Oversee the activities of critical ICT third-party service providers



Encourage the exchange of intelligence regarding ICT threats

¹ REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014

The Global Regulatory Landscape

ICT and cyber resilience remain key focus areas for supervisory authorities. While cyber resilience structures and activities currently form part of the existing regulatory landscape across ICT risk management and operational resilience, further activity to tackle increasingly complex technological threats is required.

Relevant Marketplace Movements







- The joint CPMI and IOSCO Guidance on cyber resilience for financial market infrastructures
- European Union Network and Information Security Directive (NIS2)
- US Securities and Exchange Commission 'Cybersecurity and Resiliency Observations'
- Central Bank of Ireland (CBI) Cross Industry Guidance on Operational Resilience
- Prudential Regulatory Authority (PRA), Financial Conduct Authority (FCA) and Bank of England Joint Policy Statement on Operational Resilience.

DORA and the CBI Perspective on Operational Resilience

While the CBI Guidance on Operational Resilience focuses on strengthening resilience against operational disruptions that impact a firm's critical or important business services, DORA prescribes specific requirements regarding operational resilience from a technological perspective. The scope of application is also much broader and there are specific technical requirements of the key obligation areas set out in DORA.

Scope of Application

While the scope of the CBI Guidance on Operational Resilience applies to all regulated financial service providers, the scope of DORA is much broader and as such, a vast range of entities from large and complex organisations to small and simple businesses may be required to comply with this regulation. Some of the types entities that are not traditionally regulated financial service providers are outlined below.

 Crypto-asset service providers	 Data reporting service providers
 Central counterparties	 Statutory auditors and audit firms
 Trade venues and repositories	 Crowd funding service providers
 Management companies	 ICT third party service providers

Key Obligation Areas

There is a considerable amount of overlap between DORA and existing regulations that are currently in place, however, DORA sets out specific and technical requirements across key obligations in the following areas, proportionate to a firm's size, business and risk profile:

 ICT Risk Management	Adopt ICT governance and control frameworks, including an IT risk management framework to be documented and reviewed at least yearly.
 ICT Incident Reporting	Streamline ICT incident reporting through the logging and classification of ICT incidents and reporting of major incidents to competent authorities using common templates and procedures.
 Digital Operational Resilience Testing	Performance of basic digital operational resilience testing at least yearly for all financial entities, and advanced threat-led penetration testing at least every 3 years for 'significant' financial entities.
 Management of ICT Third-Party Risk	Monitor third-party contractual arrangements at all stages and enable European Supervisory Authorities (ESAs) oversight of ICT third-party service providers deemed 'critical'.
 Information-Sharing Arrangements	Voluntary participation in intelligence sharing through the exchange of cyber threat information among financial entities, including tactics, procedures and signs of compromise.

Next Steps

Once the legislation is finalised, which is expected during 2022, it will need to be passed into law by each EU member state and the relevant European Supervisory Authorities (ESAs) including the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Occupation Pension Authority (EIOPA) will develop technical standards for financial entities to abide by.

Once entered into force, the requirements will apply 12 months after the date of entry, with Articles 23 and 24 (relating to regulatory technical standards for threat-led penetration testing) applicable 36 months after the date of entry. It is important that firms begin to evaluate the impact of this regulatory change on their ICT risk management framework, and prepare to meet the specific requirements set out by DORA. Key next steps for your organisation to consider are set out below.

01. | Establish a DORA programme and appoint a programme director and sponsor
02. | Develop a DORA board positioning paper
03. | Define a Terms of Reference and build a business case to mobilise the DORA programme
04. | Establish a governance forum and understanding where the DORA programme interacts with broader firm initiatives
05. | Mobilisation of the design phase of the DORA programme

How KPMG can help

Our team also has deep technical expertise across the Digital Operational Resilience obligation areas including ICT Risk Management, ICT and Cyber Resilience and Incident Management, ICT Third Party Risk Management in addition to broad Governance, Risk and Compliance skills. We have also supported numerous clients on their broader Operational Resilience journeys over the last number of years.

Assessment or definition of your Digital Resilience Strategy

Determining the level of your Digital Resilience Maturity based on the existing landscape

Assessment of your Digital Resilience Programme to provide assurance and ensure compliance

Assessment of your ICT Risk Management Framework and supporting processes

Operating Model Design for the management of Digital Resilience across the organisation

Development of an Implementation Roadmap for your DORA Programme

Assessment of Digital Resilience Testing currently in place

Assessment of your ICT Third Party Risk Management processes



OWEN LEWIS

Partner & Head of Management Consulting in KPMG Ireland

T: +353 87 050 4760

E: owen.lewis@kpmg.ie



DANI MICHAUX

Partner and EMA Cyber Lead, in KPMG Ireland

T: +353 87 050 4769

E: dani.michaux@kpmg.ie



IAN NELSON

Partner & Head of Regulatory, Head of Banking & Capital Markets in KPMG Ireland

T: +353 87 744 1989

E: ian.nelson@kpmg.ie



JACKIE HENNESSY

Partner, Technology Risk, Risk Consulting, in KPMG Ireland

T: +353 87 111 5970

E: jackie.hennessy@kpmg.ie



PATRICK FARRELL

Partner, Risk Consulting, in KPMG Ireland

T: +353 1700 4029

E: patrick.farrell@kpmg.ie



HERMES PERAZA

Director, Risk Consulting, in KPMG Ireland

T: +353 87 744 1981

E: hermes.peraza@kpmg.ie



DAVID POLLEY

Director, Management Consulting, Regulatory Driven Transformation, in KPMG Ireland

T: +353 87 111 5970

E: david.polley@kpmg.ie



MATTHEW GREEN

Director, Regulatory, in KPMG Ireland

T: +353 87 050 4377

E: matthew.green@kpmg.ie



CARMEN CRONJE

Associate Director, Risk Consulting, in KPMG Ireland

T: +353 87 050 4455

E: carmen.cronje@kpmg.ie



© 2022 KPMG, an Irish partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks of KPMG International Limited ("KPMG International"), a private English company limited by guarantee.

If you've received this communication directly from KPMG, it is because we hold your name and company details for the purpose of keeping you informed on a range of business issues and the services we provide. If you would like us to delete this information from our records and would prefer not to receive any further updates from us please contact unsubscribe@kpmg.ie.

Produced by: KPMG's Creative Services. Publication Date: February 2022. (7926)