KPMG

DORA decoded

Your gateway to digital resilience in financial landscapes

Digital Trust

July 2024

kpmg.com/in

KPMG. Make the Difference.

DORA: Enhancing digital resilience

The Digital Operational Resilience Act (DORA), implemented by the EU, strengthens the financial sector's resilience in the digital era. Effective from January 2025, it mandates robust cybersecurity measures, incident response plans, and reporting obligations for financial institutions. Co-operation among stakeholders is encouraged to bolster collective cyber resilience. DORA creates a regulatory framework whereby the financial firms will have to make sure they can withstand, respond to and recover from all types of Information and Communication Technology (ICT) related disruptions and threats, with an objective to prevent and mitigate cyber threats. By setting clear requirements and promoting information sharing, DORA addresses evolving cyber threats, safeguarding financial stability.

Who is impacted?

Financial entities and their critical ICT providers are mutually dependent on each other to ensure the operational resilience of the financial sector in compliance with DORA. By working together effectively, they can strengthen cybersecurity measures, enhance incident response capabilities, and contribute to the overall stability and integrity of the financial system.

Financial providers

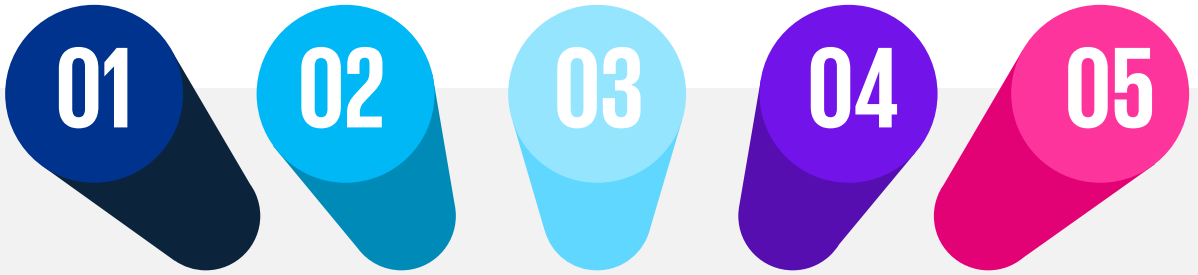
- Management companies
- Payment institutions
- Institutions for occupational retirement provision
- Secularisation repositories
- Credit institutions
- Crypto asset service providers
- Investment firms
- Trade repositories
- Central counterparts
- Data reporting service providers
- Electronic money institutions
- Admiration critical benchmarks
- Insurance/reassurance undertaking
- Central security depositories
- Insurance ancillary intermediary
- Trading venues
- Crowdfunding service providers
- Credit rating agencies
- Account information service provider
- Management of alternate investment fund

ICT providers

- Cloud computing providers
- Data processing providers
- Network connectivity providers
- Cybersecurity providers

Five pillars of DORA

The five pillars of DORA underscore critical aspects of safeguarding digital infrastructure and ensuring operational continuity in the face of evolving threats. DORA validates the effectiveness of implemented measures and identifies areas for improvement, enabling organisations to continually enhance their preparedness and response capabilities.



ICT incident management

The financial entity's management must ensure a robust ICT risk management framework, including regular testing of response and recovery activities, to minimise risks effectively.

ICT risk management

Establishes an ICT incident management process, including incident classification, monitoring, and reporting major incidents to relevant authorities, as per proposed guidelines.

Digital operational resilience testing

Implements a risk-based digital operational resilience testing program, including independent testing and internal resources, with annual testing for critical systems and triennial 'threat-led penetration testing' for non-micro financial entities.

Cyber threat information sharing

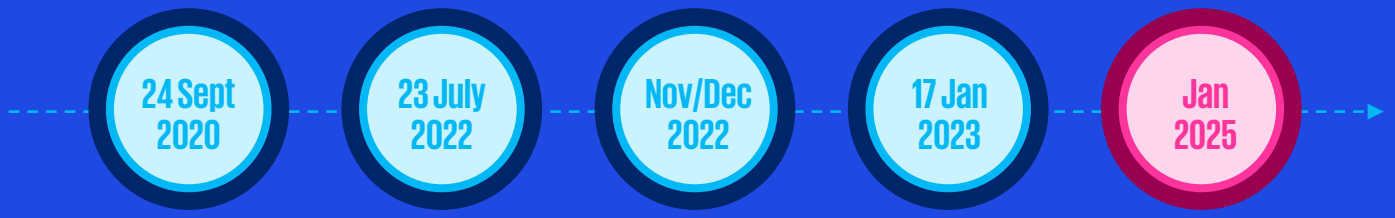
Financial entities share cyber threat information to bolster digital operational resilience, within trusted communities and in compliance with relevant laws, aiming for mutual protection.

ICT third-party risk management

Integrates ICT third-party risk into the risk management framework, including strategy adoption, maintaining a register of contracts, and conducting assessments as per European Supervisory Authorities (ESA) requirements.

Timeline

Emerging as a pivotal framework within the European Union, DORA charts a course towards a reinforced digital fortitude. It paves a way for cultivating a resilient and interconnected digital landscape, equipped to navigate the complexities of modern challenges.



Publication of DORA proposal by European Commission

Provisional agreement on DORA

Publication of DORA in the Official Journal of EU

Adoption day: DORA comes into force

Compliance with DORA and its technical requirements

Key challenges

Navigating the key challenges in implementing DORA present significant hurdles for organisations across various sectors as follows:

01

Monitoring ICT third-party risk. Service providers can be placed under the control of competent authorities. Reporting of serious incidents, which requires a rapid, efficient and comprehensive response capability.

02

Complexity in a harmonised ICT risk management framework and management design increases significantly, considering market participants and all relevant risks and scenarios. This means increased testing requirements - especially for the execution of threat led penetration testing.

03

DORA interfaces with various security disciplines, including IT operations, Information Security Management (ISM)/ Information Risk Management (IRM), Crisis Management, Business Continuity Management (BCM) / IT Service Management (ITSM) and outsourcing. Alignment of security disciplines & interfaces to ensure optimal resilience in operational business can be challenging.

04

Overlap of incident reporting as mandated by DORA and Network and Information Security Directive (NIS-2).

Our approach

Context workshop – Understanding DORA - KPMG in India will conduct workshops with organisations' stakeholders to arrive at a final scope and DORA applicability

Implementation roadmap – KPMG in India will create a roadmap categorising the identified gaps and non-compliance based on severity and implementation time

DORA

As-is gap assessment – KPMG in India will conduct As-is gap assessment of the resilience posture of the organisation and provide recommendations

Implementation assistance – KPMG in India will document policies, procedures and controls in line with the recommendations to ensure compliance with the act

Why KPMG in India?

01

KPMG in India: DORA regulation expertise

KPMG in India excels in DORA regulation disciplines, offering consulting ISM, IRM, BCM, outsourcing, and cloud solutions to support clients extensively.

02

Expertise in control management and risk assessment

With a profound understanding of processes, risks, controls, and governance structures, we provide expert support for effective control and risk management.

03

Industry tailored solution

KPMG in India provides extensive project experience in the industry and valuable insights, enabling them to understand clients' challenges and develop custom services tailored to their specific needs.

04

Global expertise for financial sector solution

Access to global expertise for financial services through our extensive global network of member firms, collaborating closely with international teams to tailor services for the sector.

05

GRC tool implementation and vendor management

We offer expertise in implementing market standard GRC tools for efficient risk and control management, along with tools for effective third-party vendor management in the ICT domain.

KPMG in India contacts:

Atul Gupta
Partner and Head
Digital Trust and Cyber
M: +91 124 336 9065
E: atulgupta@kpmg.com

Nitin Shah
Partner
Digital Trust
M: +91 124 336 9062
E: nitinshah@kpmg.com

Merril Cherian
Partner
Digital Trust
M: +91 80 6833 5524
E: mcherian@kpmg.com

Akanksha Saxena
Director
Digital Trust
M: +91 9910116342
E: akankshasaxena@kpmg.com

kpmg.com/in

Access our latest insights
on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.