KPMG

The EU Digital Operational Resilience Act (DORA)

Act Now: 5 practical steps to improve your resilience and get ready for DORA

June 2024

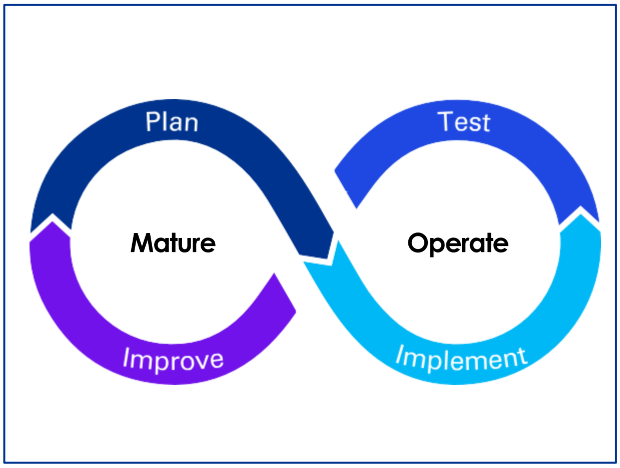
Getting DORA-ready

What does DORA readiness mean for you? Financial sector entities have been focused on ICT risk management and compliance and their respect to resilience for a number of years.

With the upcoming DORA regulation, entities must move from preparation to implementation and take steps towards demonstrating how their practices comply with DORA.

Financial entities will need to demonstrate appropriate security and resilience of critical ICT systems and applications to comply with DORA. The level of compliance efforts will vary depending on the size and complexity of your entity. A risk-based approach, appropriate security and resilience testing are necessary to address potential vulnerabilities and to prove compliance in meeting evidence requirements of the European Supervisory Authorities. By focusing on long-term resilience, entities can establish a resilient foundation, which will aid them in their steps towards DORA compliance.

Resilience means learning from the past, to improve the present, and to prepare for the future.



Our 5 key actions towards DORA readiness

In order to make entities ready for DORA, we have identified 5 key actions to assist those that are in the preparation phase. These actions will enable entities to effectively manage their digital operational resilience and be ready for DORA:

1. Determine strategic priorities and set up a DORA implementation program
2. Implement resilience and incident management measures to effectively manage continuity risks
3. Manage third party risks
4. Test digital operational resilience
5. Implement (additional) measures for resilience and ICT incident handling

Action

Determine strategic priorities and set up a DORA implementation program

How do I ensure that in the long-term my digital operations are resilience and in line with good practice requirements?

What is my (end-state) vision for our digital environment taking to heart the objectives of DORA?

Relevant DORA Pillars:

ICT Risk Management

The approach

Key stakeholders

CIO, CISO, COO, Head of (IT) Risk, CRO, Legal & Compliance Officer, BCM/Resilience coordinator

What does my business need?

- ✓ An integrated digital operational resilience strategy that is carried throughout the organisation.
- ✓ A long-term resilience program.

Objective

To enhance your daily business practices, aim to achieve a transformation towards a resilient end-to-end IT & operations environment. In order to ensure strong risk management, be focused on achieving a broad agile transformation that takes into account risks associated with your ICT/technology suppliers and continuity measures. Additionally, it is necessary to aim to increase your agility in serving digital channels by implementing strong BCM measures.

Key success factors

- Managerial support and vision for the long-term.
- Good communication for awareness of affected stakeholders.

Action

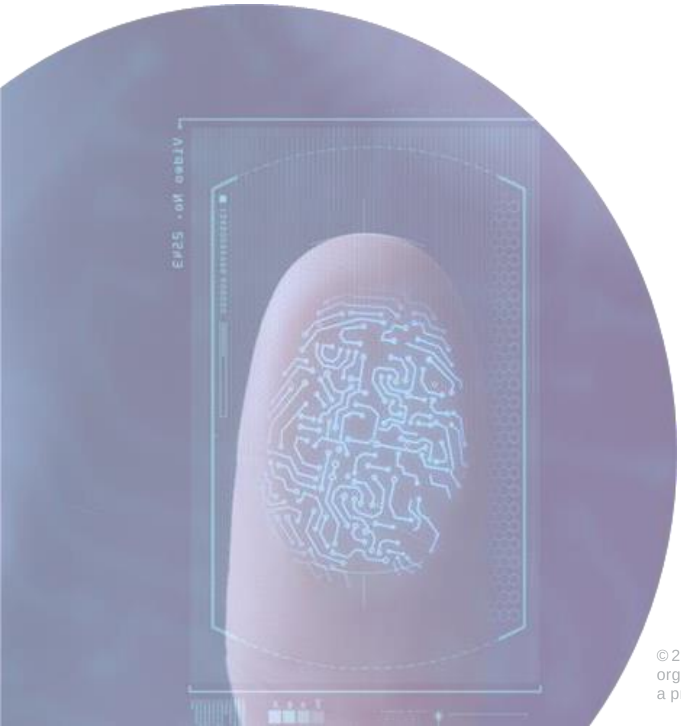
Implement resilience and incident management measures to effectively manage continuity risks

What are my key risks that threaten my digital operational resilience – and what can I do to manage them effectively?

Relevant DORA Pillars:

ICT Risk Management

Information Sharing



The approach

Key stakeholders

BCM/Resilience coordinator, CISO, COO, IT and Security Management, First-line management functions

What does my business need?

- ✓ Mapping of current gaps with good practices and DORA requirements.
- ✓ Defines measures and implementation roadmap, including effective follow-up measures on chosen activities.

Objective

To ensure effective implementation of your program, it is crucial to ensure leadership support, as well as translation of strategic and regulatory requirements into operational measures.

It is essential to enable control owners and line management to manage compliance requirements in a risk-based way, including the automation of controls related to digital resilience, in order to manage the complexity of (compliance) requirements effectively.

Think big and start small – for example, by organising a workshop with relevant middle-management players to align and agree on the implementation strategy of your DORA program.

Key success factors

- Focus on actualising long-term resilience, not just on compliance.
- Leadership support and involvement.

Action

Manage third party risks

How well is my understanding of my ICT supply chain?

To what extent does my business have a central contract management administration for supporting the third party life cycle?

Has my business prepared exit strategies for their current ICT third parties to ensure smooth continuation of their business and ICT processes in case service delivery is discontinued by an ICT third party?

Relevant DORA Pillars:

Third Party Risk Management

The approach

Key stakeholders

CIO, CISO, COO, Legal & Procurement Officer

What does my business need?

✓ A strong and transparent TPRM management structure, with extensive policies, procedures and monitoring force.

Objective

To ensure effective management of ICT risk related to third party providers, it is essential to conduct complete monitoring of all ICT-related third party risks throughout all relationship phases.

This involves the classification and analysis of providers and their management bodies, record-keeping of relevant information, managing proportionality, managing compliance, and creating a TPRM risk strategy. By undertaking these steps, comprehensive management of ICT risk in relation to third party providers can be ensured.

Key success factors

- Active TPRM throughout the whole third party lifecycle (strategy – governance - pre-contract – contracting – contract management & business as usual).
- Avoiding ICT concentration risk at entity level.

Action

Test digital operational resilience

Does my business perform digital resilience testing on a regular basis to stay resilience in light of cyber threats?

Does my business have process in place to prioritise penetration testing though risk and threat assessments?

Relevant DORA Pillars:

Digital Operational Resilience Testing

The approach

Key stakeholders

CISO, IT Management, CRO

What does my business need?

- ✓ All critical ICT systems & applications are tested at least once per year by an independent party.
- ✓ The testing program is risk-based.

Objective

To ensure operational resilience, it is crucial to test critical and important functions more frequently than non-critical or unimportant function, at least once per year.

The program for testing digital operational resilience must be based on relevant threat scenarios. Best practice is to implement an appropriate test set-up for each threat, in order to test the resilience effectively. Moreover, every three years, entities are required to perform Threat-Lead Penetration Testing (TPLT) hat simulates a realistic and advanced cyber attack. This simulation helps organisation prepare and train for real cyber attacks.

Key success factors

Action

Implement (additional) measures for resilience & ICT incident handling

How strong is my business's ICT incident handling?

If my business experiences a major IT incident, are you able to continue operations in the meantime and recover swiftly?

How does my business report major security incidents to the national authorities?

Does my business exchange cyber-threat information with other (peer) entities?

How do I do effective cyber threat management?

Relevant DORA Pillars:

ICT Incident Management

Digital Operational Resilience Testing

The approach

Key stakeholders

CIO, CISO, COO, SOC & IT Managers

What does my business need?

- ✓ A strong incident reporting structure.
- ✓ Cross-organisational awareness for resilience.

Objective

To establish strong operational resilience measures and incident management, it is essential to accomplish resilience testing from a wider perspective, which – beyond technical security testing – includes regular crisis simulations.

It is important to improve business continuity plans and ICT crisis scenarios to ensure that uncontrolled disruptions are avoided due to slow and ineffective incident management.

Moreover, accomplishing mature threat intelligence and assessing top continuity risk scenarios is crucial to enhance resilience and preparedness in critical situations.

By understanding these measures, strong operational resilience can be established, ensuring smooth and uninterrupted operations.

Key success factors

- Have clear communication lines and reporting processes.
- A security-awareness culture that encourages early reporting of incidents.

What we do

Assess

- ✓ Gap analysis to assess DORA compliance
- ✓ Compliance roadmap development

Design

- ✓ DORA program support via program design, governance and assurance
- ✓ Target Operating Model (TOM) design

Deliver

- ✓ Technical remediation support across ICT risk management, infrastructure, business continuity, IAM, digital testing, incident management and third-party risk
- ✓ People and change management via training, skills plans, communication packs etc.

Monitor

- ✓ Technology enablement
- ✓ Compliance programme to ensure future alignment
- ✓ Internal audit DORA support

DORA compliance assessment baselining

Subject matter experts and DORA Program support

Advisory, audit and assurance services

Aligned with client business priorities and needs

Your contacts

Jackie Hennessy
Partner, Technology Risk Consulting
KPMG Ireland
e: jackie.hennessy@kpmg.ie

Dani Michaux
EMA Cyber Lead
KPMG Ireland
e: dani.michaux@kpmg.ie

Michelle Byrne
Director, Technology Risk Consulting
KPMG Ireland
e: michelle.byrne@kpmg.ie

Carmen Cronje
Director, Technology Risk Consulting
KPMG Ireland
e: carmen.cronje@kpmg.ie

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.

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.

Credits: This document has been created through the collaborative efforts with KPMG Netherlands

Publication Date: June 2024. (10515)