REPORT

xceedance
Your way forward

Digital Operational Resilience Act

How to get ready for DORA

Introduction

In July 2024, a faulty update by an unfortunate vendor caused an IT outage of such significant magnitude that it was felt throughout the world. This outage exposed the importance of improving operational resilience in an robust and strategic way.

Operational resilience is often seen as a background concern, and not given proper care and attention. However, the degree of operational resilience that an organization can achieve through the application of a robust technology design is incredibly high.

In the case of the July 2024 incident, many organisations had either relied upon the downstream operational resilience of their public cloud provider; and/or decided against spreading risk across multiple clouds; and/or had not considered cloud outage within their disaster-recovery processes. The impact of this one outage, and the consequential losses made on that day, will certainly have led many to urgently reconsider their business continuity plans.

Perhaps this was the type of incident predicted by the EU when its members began drawing up the Digital Operational Resilience Act ("DORA") – and perhaps they simply wanted to protect the financial services sector, including the insurance sector, which is of critical importance to the global economy.

DORA's principal aim is to ensure that the financial services sector is resilient against IT, Cyber and Digital threats. The regulation sets out standards for the sector designed to harmonise rules, ensure that the highest standards of IT governance and risk management are met, and encourage investment in the requisite systems.

This article provides an overview of the DORA legislation, its aims and its application, as well as detailing how insurance businesses can prepare for DORA's implementation, and what actions they can take now to ensure a smooth transition.

JARNO SEEGERS

Vice President,
Business Development Executive EMEA

jarno.seegers@xceedance.com
www.xceedance.com

The Basics

What is DORA? What does it say?

The Digital Operations Resilience Act (DORA) is a European law, that is designed to protect financial institutions from cyber threats. It ensures banks, insurance companies, and other financial services providers are prepared and equipped to handle digital risks well.

DORA requires that financial services institutions have robust systems in place to prevent, detect, and recover from cyberattacks adequately. DORA also promotes cooperation across the financial sector, stipulates that businesses regularly test their digital security and report incidents.

Overall, the act aims to make the financial system more resilient, safer and more reliable in an increasingly digital world.

Application & Jurisdiction

DORA applies across the European Union and affects a wide range of financial institutions, including banks, insurance companies, investment firms, and payment service providers. It also applies to third party service providers that offer digital and information and communications technology (ICT) services to those financial institutions, such as cloud computing providers.

DORA primarily applies within the EU. However, its impact is likely to extend beyond those boundaries because non-EU companies that provide digital or financial services to EU-based institutions must also comply with the law.

All UK-based financial services entities that have market activities within the EU, as well as their 'Critical ICT Third Party Providers' (CTTPS) are subject to the requirements. There are no specific requirements prescribed in relation to company size or turnover.

The deadline for DORA compliance is 17th January 2025.

In order to reach a global standard, regulations covering the same subject matter will likely be developed in other key insurance hubs, such as Zurich, Singapore, and the US.

Benefits of compliance:

Whilst there is a legal requirement to comply with the DORA regulations, there is also a range of other benefits for insurance businesses:

Enhanced Cyber Security – by enforcing robust security measures, DORA will help better protect against cyber threats, reducing the risk of data breaches and system disruptions.

Operational Resilience – institutions are required to establish strong systems for identifying, managing, and recovering from digital risks, ensuring business continuity even during cyber incidents or technical failures.

Increased Trust – compliance with DORA builds customer and stakeholder confidence, as it demonstrates that the institution prioritizes security and has safeguards in place to protect financial and digital assets.

Consequences of getting it wrong:

Failure to comply with the regulations could result in some significant consequences, including but not limited to:

Financial Penalties – regulatory authorities can impose financial penalties on institutions that fail to meet DORA's requirements, which will likely vary depending on the severity of the breach.

Operational Restrictions – financial institutions may face limitations on their operations, or even suspension of certain services, if they are found to be non-compliant.

Reputational Damage – non-compliance can harm the institution's reputation, eroding customer trust and leading to potential loss of business or market share.

Readiness

Understanding DORA's requirements:

Many financial services firms already have robust systems and processes in place to cover other regulatory commitments, such as ISO 27001. Therefore, a key aspect of ensuring compliance with the DORA regulations will be conducting a GAP analysis; evidencing compliance where it already exists; and developing and implementing a plan of action where attention is required.

The key requirements outlined in the act are:

Threat and Vulnerability Management – including penetration testing at least every three years.

Service Availability – having continuity plans in place that ensure businesses will be able to continue services during disruptions.

Regularly addressing risks relating to market operations and financial stability.

Governance and Culture – establishing a resilient culture and governance framework.

Third Party Dependencies – managing the risk within the supply-chain, much more than simply outsourcing the risk to a third-party.

What needs to be assessed?

IT Governance: to accommodate an update to the existing rules.

IT Risk Management: to fully understand the pre-requisite IT risk management principles.

IT Incident Reporting and analysis: to consider how incidents can be reduced or stopped.

Digital Operational Resilience Testing.

IT Third-Party Management: to ensure that due diligence extends to suppliers and across the entire supply chain.

Reporting: to ensure compliance, conduct a thorough audit of reporting processes.

Action

With DORA in full force in less than six months' time, the time has come to develop and implement a comprehensive action plan to ensure compliance. Consider the following five-part outline:

Phase One: Discovery & Planning

Assess current policies and identify gaps in compliance, e.g. incidents, project and change policy, governance and organisation, information security policy, asset management, risk framework, physical security, access and identity controls, ICT operations security, data and network security, systems development and maintenance, business continuity. Review and understand ICT risk management policy and IT management policies to build a list of known gaps. Establish digital operational resilience testing plans. Speak with third-party suppliers to understand their risk management policies and operational risk frameworks.

Phase Two: Impact Analysis

Review any significant incidents and cyber threats and develop a system to classify them by establishing definitions and categories (e.g. reputational impact, duration/downtime, geographical region(s), data loss, critical service impact, economic impact, etc.) to assist in any required reporting.

Phase Three: Planning

Develop a comprehensive plan of action based upon phase one findings and phase two classifications. Include a time frame and principal responsible team members for each action.

Part Four: Register of information

Create a register which lists your documented findings, decisions and changes (e.g. information register, general requirements statement, defined scope of recommended changes, defined material external services, minimum requirements).

Part Five: Execution

Work with ICT services and supporting critical functions (e.g. policy and commercial review – risk profile and complexity, governance changes for service providers running critical functions, contractual changes and monitoring, due diligence) to implement required changes. Have a clear pathway, timeframe and team responsible for delivery.

At the end of the project, businesses should be able to evidence that they meet all requirements in the DORA regulations, and should keep this information on record along with their plan of action in order to rerun the project on a regular basis to ensure continuing compliance with DORA as well as the incorporation of stakeholder feedback.

Next Steps

To ensure a smooth transition to DORA compliance, insurers need to take a proactive and strategic approach. As a priority, businesses should conduct a GAP analysis, strengthen governance and risk management, engage with third-party providers, develop incident reporting protocols, implement continuous monitoring systems, and prepare for regulatory engagement.

It's time to act.

The Xceedance Edge

Xceedance is an insurance service provider that empowers global insurance organisations with strategic operations support, innovative technology, and data-driven insights. With a 100% focus on the insurance industry, Xceedance offers unique insights and support to clients across the insurance value chain.

The goal is to ensure digital resilience throughout the EU's financial sector, safeguarding it from cyber risks and operational disruptions.

Learn how Xceedance can help your organization navigate complex market challenges, manage rapidly-evolving policyholder expectations, boost regulatory compliance, and kickstart enterprise transformation. Ready to find your way forward? Reach out to us at **contact@xceedance.com** to get started.

Scan the QR code to visit our website, or go to www.xceedance.com

xceedance