XM Cyber

Adopting DORA with XM Cyber Checklist

Financial institutions must uphold high standards of service, continuity, and resilience to protect data and combat cyber threats, while at the same time delivering innovation in secure digital services to drive growth, achieve differentiation, and build trust with both their customers and partners.

The evolving threat landscape demands constant adaptation of cyber defenses and the implementation of robust security processes.

The Digital Operational Resilience Act (DORA), has been designed to help Financial institutions address these growing challenges.

What is DORA, Why is it important, What should we do?

The Digital Operational Resilience Act (Regulation (EU) 2022/2554) addresses the topic of digital operational resilience for financial services. DORA represents the EU’s most important regulatory initiative on operational resilience and cybersecurity.

DORA has been designed to help Financial institutions maintain full control over Information and Communication Technology (ICT) risk, to establish comprehensive capabilities that have a positive effective on ICT risk management. It also addresses specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. Likewise, it looks at how financial institutes should have policies in place for the testing of ICT systems, controls, and processes, as well as for managing ICT third-party risk.

Steps to Success in Adopting DORA Checklist:

The steps outlined in the following pages are a summary of the key steps to success, as they align to the 5 key pillars of the DORA regulation.

CHAPTER II

ICT Risk Management:

□ **Document critical ICT Assets and Business functions:** Identify Critical Assets and align them to classification groups based on criticality levels.

□ **Initiate a Gap Analysis and document findings:** Discover exposure risks and weaknesses in security defense that could impact the integrity and availability of ICT systems and services.

□ **Define risk appetite and tolerance levels:** Monitor detection thresholds and related processes to ensure they remain in line with desired tolerance.

□ **Implement resilience of business-critical systems:** Ensure the safety, security, availability, integrity, backup, and recovery of ICT systems and data.

□ **Establish a continuous learning and evolution cadence:** To regularly review and optimize your ICT Risk Management Framework.

CHAPTER III

ICT-Related Incident Management, Classification and Reporting:

□ **Establish a comprehensive incident management and response strategy:** That encompasses technology, people, and processes for both incidents and cyber threats.

□ **Streamline the process to detect, log, and classify all ICT-related incidents:** With clear information-gathering requirements and a documented reporting cadence.

□ **Define thresholds for incident classification levels:** Minor and major incidents, along with critical breach. Criteria to consider include: quantification of affect, duration & downtime, critical services affected, geographic spread and economic impact.

□ **Define cyber threat categorization and impact analysis process:** Including likelihood, and business impact, based on the predicted affect on critical systems and business operations.

□ **Harmonize and evolve ICT management processes:** To regularly review and optimize your ICT-related incident management and reporting processes.

CHAPTER IV

Digital Operational Resilience Testing:

□ **Define the scope of your DORA testing cadence:** That includes systems, tools, protocols, processes, and attack surfaces. Incorporate a preparedness analysis.

□ **Initiate a DORA testing cadence for ICT Risk:** Conduct regular and comprehensive testing for all ICT exposure risks, across all attack surfaces.

□ **Initiate a DORA testing cadence for Security Defenses:** Conduct regular and comprehensive testing for all security defenses and threat detection solutions.

□ **Initiate a DORA testing cadence for Incident Management Processes:** Conduct regular testing of ICT-related Incident Management Processes, systems and response measures.

□ **Prepare for Threat-Led Penetration Testing:** Select suitable partners and tools in order to implement a Threat-Led Penetration Testing (TLPT) cadence. Incorporate a preparedness analysis of all attack surfaces.

CHAPTER V

ICT Third-Party Risk Management:

□ **Create a register of third-party ICT-related service providers:** Document and report a complete register of third-parties including outsourced activities and the risk they may pose to digital services and resilience.

□ **Declare which of the above provides critical ICT services:** Specify which third-parties deliver services deemed critical to the operation of the business.

□ **Define Oversight committee, with roles and responsibilities:** Review the requirements of the Lead Overseer for each ICT-related service provider.

□ **Initiate DORA testing cadence for ICT-related third-party risk:** Conduct regular testing of ICT-related service providers, in line with your ICT risk management framework.

□ **Harmonize processes and communication with partners:** Work with ICT-related service providers to continually learn and evolve risk analysis, testing, and communication processes.

CHAPTER IV

Information Sharing Arrangements:

□ **Establish a GRC project team for DORA:** Extend your Governance, Risk, and Compliance teams and processes to incorporate and manage the DORA program and framework.

□ **Foster a culture of intelligence sharing:** With industry counterparts, partners, and third-party ICT-related service providers.

□ **Select qualified and reputable partners for consultative support and guidance:** Establish a bi-directional information sharing and communication flow.

□ **Stay informed and up to date with DORA requirements:** Establish a clear line of communication with regulators and authorities.

□ **Training, education, and knowledge transfer:** Ensure all team members are suitably educated on all DORA-related requirements, processes, and operational resilience measures and their evolution over time.

For more information on the Digital Operational Resilience Act (DORA), check out:
https://www.digital-operational-resilience-act.com/DORA_Articles.html

Whitepaper

DORA

Read our Whitepaper Demystifying DORA with XM Cyber

Download Now

Webinar

DORA

Watch our Demystifying DORA with XM Cyber webinar featuring KPMG

Watch Now ▶

How XM Cyber aids adoption with DORA:

Effective exposure management is crucial for financial institutions aiming to align with the Digital Operational Resilience Act. Supporting ICT Risk Management and ICT-related Incident Management with the XM Attack Graph Analysis™ to identify, prioritize and validate the exploitability of exposure across the digital attack surface. Ensures security operation teams can focus their remediation efforts and threat investigations on high-impact exposure that present the biggest risk to business-critical assets and ICT systems. To help optimize digital operational resilience and accelerate the successful adoption of DORA.

Quantification of risk using XM Attack Graph Analysis™

The risk intelligence and exposure insights provided through the platform help organizations identify & classify critical ICT assets, and quantify the risk presented by vulnerabilities, misconfiguration, weak security posture, and identity issues across their digital attack surface on a continuous basis, to optimize ICT Risk Management.

Accelerate and Enrich incident investigation to aid recovery and prevent future breaches

Holistic exposure risk intelligence and attack path insights to enrich advanced Threat Hunting and post-incident investigation. With rich contextual information reported in threat scenarios to accelerate incident investigation, and enhance the learning and evolution of the ICT-related Incident Management processes.

Simplify Digital Operational Resilience Testing

The platform delivers a comprehensive, continuous, and automated approach to support digital operational resilience testing. The XM Cyber platform delivers end-to-end testing of the external attack surface of financial entities and their third-party ICT service providers, as well internal digital attack surface testing for vulnerability assessments, security control testing, and as a continuous approach to Threat-led Penetration Testing (TLPT). To aid audit readiness, uncover risk, and prevent cyber threats.

XM Cyber is a leading Continuous Exposure Management company that transforms the way organizations approach cyber risk, enabling security teams to prevent more attacks with 75% less remediation effort. Its XM Attack Graph Analysis™ capability discovers CVEs, misconfigurations, and identity issues across on-premise and all major cloud environments. It analyzes how attackers can chain exposures together to reach critical assets, identifies key “choke points”, and provides remediation guidance. Founded by top executives from the Israeli cyber intelligence community, XM Cyber has offices in North America, Europe, Asia, and Israel.