Navigating EU Cybersecurity Regulations to Protect Critical Infrastructure and Ensure Compliance

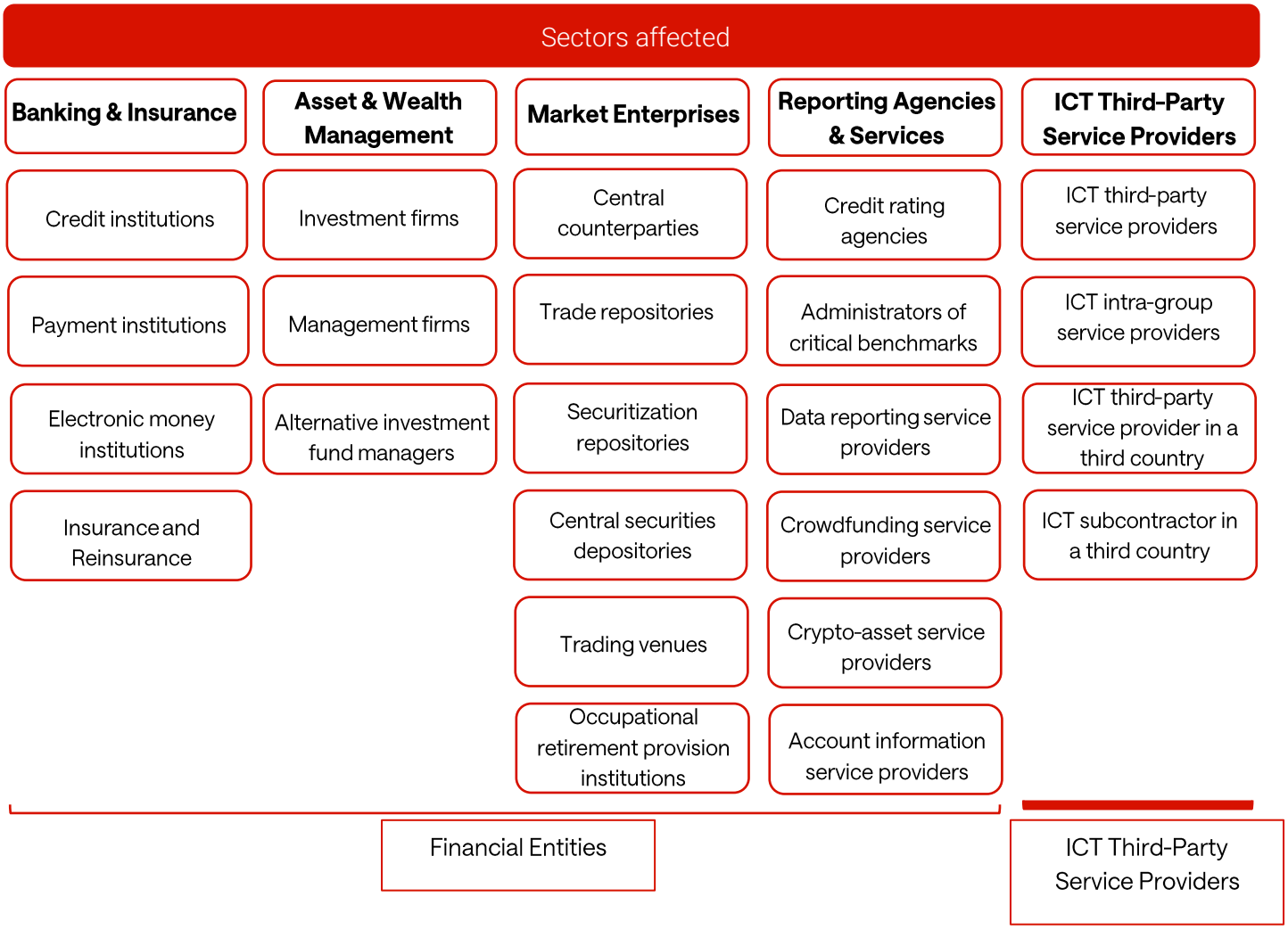
DORA Compliance Checklist

Your Checklist to Complying with DORA Guidelines

Table of Contents

Introduction

First, determine whether your organization falls within the expanded scope of the Digital Operational Resilience Regulation (DORA). DORA applies to a wide range of players in the financial sector, including insurance and reinsurance companies, alternative investment fund managers (AIFMs), and management companies. It includes both large and small companies and ensures comprehensive coverage. Directive (EU) 2022/2555 establishes a uniform criterion for determining companies that fall within the scope of DORA, the so-called size threshold. The regulation covers three types of financial undertakings.
DORA addresses issues such as cybersecurity, ICT risks, and digital operational resilience. Hence, organizations must assess their cybersecurity practices and operational resilience. National regulators such as BaFin, in Germany, are preparing for the implementation of DORA. Details: BaFin - DORA



Step 1: Understanding the Scope of Regulation

To begin, here is a comprehensive approach to the assessment of your IT systems:

☐ **Risk Assessment and Management**

Critical asset identification: Identify business-critical systems and data, and conduct regular assessments to identify potential threats and vulnerabilities and the potential impact of various cyber incidents.

☐ **Compliance with Standards and Regulations**

Ensure compliance with all DORA requirements and alignment with standards such as ISO/IEC 27001, NIST, and GDPR.

☐ **Assessment of Network and System Security**

Regular penetration testing to identify and remediate security vulnerabilities, and real-time vulnerability scanning.

☐ **Incident Response and Management**

Development and maintenance of a comprehensive contingency plan, regular simulations and exercises of the contingency plan, and testing of robust backup and recovery solutions.

☐ **Continuous Monitoring and Improvement**

Implementation of tools and processes for continuous monitoring. Internal and external audits to ensure compliance and improve KPIs and reporting mechanisms.

☐ **Employee Training and Sensitization**

Regular cybersecurity and resilience training and phishing awareness testing.

☐ **Risk Management for Third-Party Providers**

Evaluate the security and resilience of third-party providers and ensure resilience and security provisions in contracts and SLAs.

☐ **Documentation and Records**

Detailed records of all assessments, incidents, improvements, and ongoing updating of documentation.

Step 2: Reviewing Key Changes & Implications of DORA

☐ **Understand the more stringent security requirements, including risk management practices and risk appetite.**

DORA extends its scope to various players in the financial sector, including insurance and reinsurance companies, alternative investment fund managers (AIFMs), and management companies. Previously, some companies may not have been subject to similar rules, but DORA now includes them. Directive (EU) 2022/2555 introduces a uniform criterion for determining entities within the scope of DORA, the so-called “size cap rule”. This ensures uniform applicability to different types of financial organizations.

☐ **Cybersecurity, reporting, and supervisory focus.**

DORA focuses on cybersecurity, ICT risks, and digital operational resilience. Organizations must improve their cybersecurity practices and operational resilience to meet the requirements. Companies covered by DORA must comply with new reporting obligations that require them to report significant incidents, disruptions, and breaches to national authorities. National supervisory authorities will be given additional supervisory powers under DORA, enabling them to assess and enforce compliance and impose penalties where necessary.

Step 3: Regular Safety Assessments

☐ Risk Management Practices

- ICT risk control function: financial organizations must delegate responsibility for managing and monitoring ICT risks to an independent control function. This will ensure effective risk control and minimize conflicts of interest.
- ICT systems, protocols, and tools: Financial organizations should use and maintain up-to-date ICT systems, protocols, and tools that are appropriate, reliable, sufficiently capable, and technologically robust.

☐ Regular Security Assessments

- Resilience testing: financial organizations must conduct a resilience test at least once a year to assess their operational resilience.
- Threat-based penetration testing: A threat-based penetration test should be conducted at least every three years to assess vulnerabilities and potential breaches.

☐ Reporting and Compliance

- Organizations must align their ICT security policies with their digital operational resilience strategy. Regular security audits and assessments are essential to ensure compliance with DORA.

What the Law Says

Chapter II, Articles 5 to 16 DORA ICT Risk Management
Document critical ICT assets: Identify and classify critical resources.
Vulnerability analysis: Identify vulnerabilities and security gaps.
Risk appetite: Monitor thresholds to adjust them to tolerance.
Resilience: Ensure the security and recovery of ICT systems.
Continuous learning: Review and optimize risk management regularly.

Chapter III, Articles 17 to 23
Incident strategy: Consider technology, people and processes.
Detection and logging: Define requirements for information collection and reporting.
Incident classification: Establish thresholds based on impact and duration.
Threat analysis: Assess the impact on critical systems.
Process optimization: Regularly review and improve incident management.

Chapter V, Section I, Articles 28 to 30
Third-party directory: Document risks and impacts of third-party services.
Key providers: Identify key ICT service providers.
Supervisory functions: Define committee responsibilities for service providers.
Risk assessment: Check third-party providers regularly.
Process harmonization: Continuously develop risk analysis and communication.

Chapter IV, Articles 24 to 27
Test scope: Systems, tools, protocols & processes.
Risk testing: Regularly test risks and security measures.
Penetration testing: Select partners and tools for TLPT.

Chapter VI, Articles 45 and 49 Expand teams to manage the DORA program.
Information sharing: Collaborate with industry representatives and partners.

Step 4: Examining your Network & Information System

☐ Identification and Documentation

- Identify and classify your ICT business functions, information assets, roles, and dependencies.
- Properly document these elements to mitigate ICT risk.

☐ Cyber Threat and Vulnerability Assessment

- Assess the cyber threats and vulnerabilities related to your network and information systems.
- Review and update this assessment regularly to stay proactive.

☐ Resilience Testing

- Establish an appropriate and risk-based digital operational resilience testing program.
- Perform various tests such as open-source analysis, vulnerability assessments, scans, gap analysis and network security assessments.

☐ Assess Your Complete Network and Systems

- Identify and document all critical assets, including hardware, software, and data, in order to prioritize protection and resource allocation.
- Establish sound cyber hygiene practices and conducting regular employee training on cyber security threats and best practices are essential.
- Regular vulnerability scans and the prompt application of patches and updates are necessary to minimize risk.
- Developing and maintaining a comprehensive incident detection and response plan, including the establishment of monitoring systems and clear response procedures, is critical.

- Continuous security monitoring with advanced tools and technologies helps to detect and respond to threats in real-time.
- A risk management framework that includes risk assessment, mitigation, and governance policies ensures ongoing compliance and resilience.
- Incident management procedures should be in place to report incidents to the relevant authorities as required by DORA.
- Regular digital operational resilience testing, such as penetration testing and scenario-based testing, helps to identify and remediate vulnerabilities.

Step 5: Facilitating your Implementation with NDR

Through the use of machine learning (ML), Network Detection and Response (NDR) improves the ability to detect, classify, and report incidents efficiently and accurately, supporting compliance with DORA Chapter III, among others. The permanent monitoring, adaptive learning, and automated reporting of ML-based NDR systems ensure that organizations can maintain a resilient and compliant ICT infrastructure.

NDR that is based on ML and AI can significantly contribute to ensuring compliance with DORA, especially in Chapter III, which focuses on the management, classification, and reporting of ICT-related incidents. Here's how it works:

☐ **Incident Detection and Monitoring**

Automated detection and real-time monitoring: ML and AI are used in NDR systems to continuously monitor network traffic and detect unusual patterns or anomalies that could indicate security incidents.

By learning normal network behavior over time, ML models can identify deviations, such as unusual access patterns or data

exfiltration attempts, and thus detect potential threats at an early stage.

▢ Classification of Incidents

AI-powered systems can classify incidents based on detected patterns and assign them appropriate severity levels and categories (e.g. malware, phishing, DDoS attacks).

They take into account the context of the anomalies and help differentiate between false positives and real threats, improving the accuracy of incident classification.

▢ Incident Reporting

Efficient and comprehensive reporting is enabled by AI-based NDR systems that automatically generate detailed reports after an incident has been detected and classified.

These reports capture all necessary information and are formatted according to regulatory requirements.

In addition, these systems send alerts and notifications to the relevant stakeholders immediately after an incident is detected to ensure that reporting deadlines are met.

▢ Machine Learning and Adaptation

AI systems continuously improve through feedback loops, learning from past incidents and responses to increase the accuracy of detection and classification.

At the same time, ML-based NDR systems adapt to new threats by constantly analyzing new data to ensure that the organization's incident management processes remain robust and in line with evolving standards.

▢ Incident Logging

NDR systems can keep detailed logs of all detected incidents, actions taken and outcomes. These logs provide a comprehensive record for audits and regulatory reviews.

They facilitate both internal and external compliance audits and ensure that the organization can demonstrate compliance with

DORA requirements. These requirements relate to the management, classification and reporting of ICT-related incidents.

Summary

AI-powered Network Detection and Response (NDR) provides an efficient and proactive solution for network security that meets the stringent requirements of DORA.

This technology improves threat detection, shortens response times, reduces false alarms and ensures continuous compliance, making it a valuable tool for maintaining network security in regulated environments.

Organizations subject to DORA regulations should consider AI-powered NDR solutions, as they:

- detect unusual patterns and behaviors in network traffic that indicate security threats,
- are able to identify sophisticated threats such as zero-day exploits that traditional methods might miss,
- provide around-the-clock monitoring to ensure that threats are detected and responded to in real-time,
- allow automated initial responses, such as isolating affected systems,
- all of which significantly reduce response times.

AI can process and analyze large amounts of data quickly, which is particularly beneficial in large and complex network environments.

By automating routine monitoring tasks, IT and security teams can focus on more complex and strategic problems.

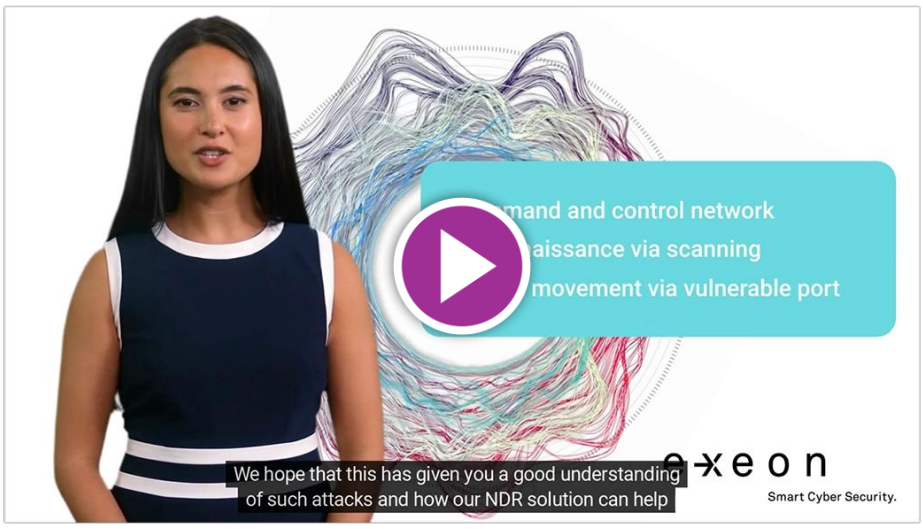
This leads to greater accuracy as AI reduces the number of false positives and puts security alerts in the right context, enabling teams to understand and respond to threats faster and more efficiently.

What Can You Do Next?

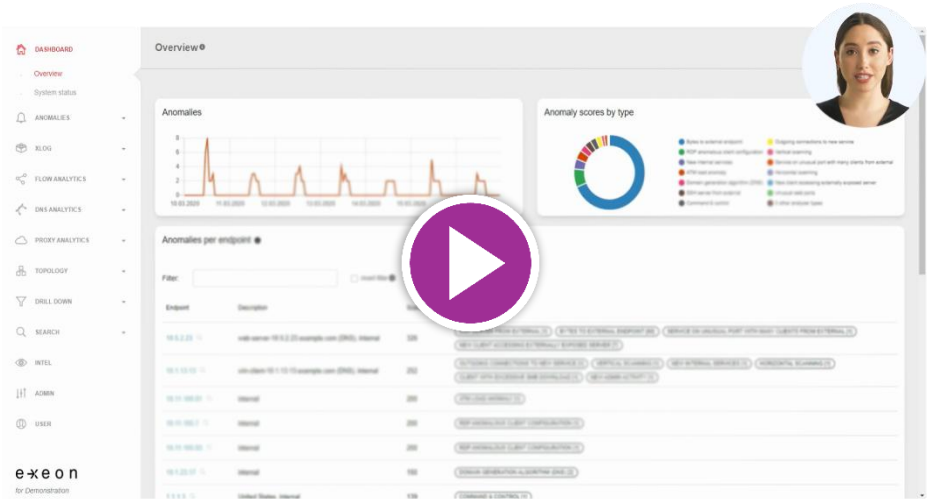
In addition to our blog containing articles on all cases and new threats happening in the real world today, we have crafted various video tours of the detection, response, and reporting of cyber threats and incidents:

AI in Action

Your Guided Tour to Threat Detection:



Monitoring ATM Machines Worldwide:



Watch the videos

Next-Gen Security Analytics, made in Switzerland. LinkedIn YouTube