XM Cyber

Whitepaper

Demystifying DORA with XM Cyber

How XM Cyber Continuous Exposure Management can help to meet the requirements of DORA

Executive Summary

Financial institutions are often regarded as technology innovators and thought leaders when it comes to the delivery of secure digital services. As such they continually strive to establish trust among their customers, stakeholders, and business partners. To do this, it is essential they maintain the highest standards of service delivery, business continuity and operational resilience. To minimize downtime, while also ensuring the safety, security, and integrity of customer data and financial records.

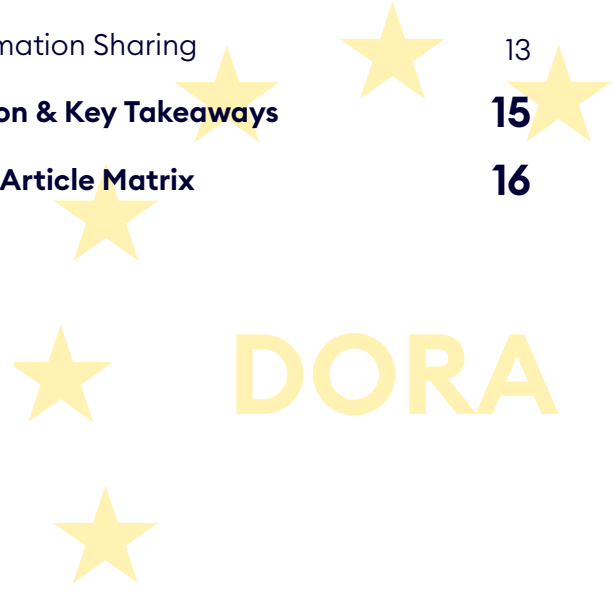
These Financial institutions are also subject to constant and persistent cyber threats, against their digital attack surface. This further compounds the need to embed comprehensive and robust security processes into the day-to-day operating cadence, of all elements of the institution.

The Threat Landscape is ever-evolving, forcing the need to continuously adapt and improve security posture, refine operational cadence, and bolster cybersecurity defenses. This ongoing need to implement effective security requires synergy between people, processes, and technology, which is not as simple as it sounds. Ensuring that each of these components are operating effectively, and aligned to the same outcomes, requires a logical structure, extensive planning, and clear objectives.

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

In this whitepaper we will introduce the key requirements for DORA, and how XM Cybers Continuous Exposure Management Platform can help your organization optimize ICT systems, people, and processes to meet the requirements.

Table of Contents



What is the Digital Operation Resilience Act (DORA)?

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) assets, to establish comprehensive capabilities that have a positive effective ICT risk management. As well as specific mechanisms and policies for handling all ICT-related incidents and for reporting major ICT-related incidents. Likewise, 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.

It aims to strengthen the IT security of, and to optimize the digital operational resilience of financial services through a continuous, end-to-end cybersecurity lifecycle, that incorporates proactive risk prevention and defensive protection, detection and containment of threats, through to incident response and recovery processes for post-breach analysis and triage, ensuring that Europe's financial sector can withstand, and recover from all types of ICT-related disruptions and threats such as cyber-attacks.

Why is DORA needed, and what does it cover?

With DORA, the EU aims to establish a universal framework for managing and mitigating ICT risk in the financial sector. By harmonizing risk management rules across the EU, DORA seeks to remove the gaps, overlaps, and conflicts that could arise between disparate regulations in different EU states. It will require firms to adopt a broader business view of resilience, with accountability established at the senior management level. The regulation came into force at the beginning of 2023. As of January 2025, DORA will be mandatory in all EU member states. Affected Companies should proactively prepare for the implementation of DORA: Perform gap analysis: Assess the current situation regarding governance, risk management, and compliance with existing guidelines and standards.

Concerning financial penalties, entities found to violate the Act's requirements may face fines. The fine will depend on the severity of the violation and the financial entity's cooperation with authorities. Financial entities that fail to report major ICT-related incidents or significant cyber threats as required under DORA may also face fines. While reporting and notification of major ICT-related incidents are voluntary to the competent authorities, major operational or security payment-related incidents must be reported (DORA article 1, ii & iii).

Who must comply with the Digital Operational Resilience Act (DORA)?

According to Article 2 (Scope) of the Digital Operational Resilience Act (DORA), this Regulation applies to the following entities:

(a) credit institutions;
(b) payment institutions, including payment institutions exempted pursuant to Directive (EU) 2015/2366;
(c) account information service providers;
(d electronic money institutions, including electronic money institutions exempted pursuant to Directive 2009/110/EC;
(e) investment firms;
(f) crypto-asset service providers as authorised under a Regulation of the European Parliament and of the Council on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 ('the Regulation on markets in crypto-assets') and issuers of asset-referenced tokens;
(g) central securities depositories;
(h) central counterparties;
(i) trading venues;
(j) trade repositories;
(k) managers of alternative investment funds;
(l) management companies;
(m) data reporting service providers;
(n) insurance and reinsurance undertakings;
(o) insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries;
(p) institutions for occupational retirement provision;
(q) credit rating agencies;
(r) administrators of critical benchmarks;
(s) crowdfunding service providers;
(t) securitisation repositories;
(u) ICT third-party service providers.

For the purposes of this Regulation, entities referred to in paragraph 1, points (a) to (t), shall collectively be referred to as 'financial entities'.

XM Cyber

Addressing the 5 key Pillars of DORA

XM Cyber Recommended Steps to Success

CHAPTER II
ICT Risk Management

1. **Document critical ICT Assets and Business functions:** Identify Critical Assets and align them to classification groups based on criticality levels.
2. **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.
3. **Define risk appetite and tolerance levels:** Monitor detection thresholds and related processes to ensure they remain in line with desired tolerance.
4. **Implement resilience of business-critical systems:** Ensure the safety, security, availability, integrity, backup, and recovery of ICT systems and Data.
5. **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

6. **Establish a comprehensive incident management and response strategy:** That encompasses technology, people, and processes for both Incidents and Cyber threats.
7. **Streamline the process to detect, log, and classify all ICT-related incidents:** With clear information-gathering requirements and a documented reporting cadence.
8. **Define thresholds for Incident classification levels:** Criteria to consider include, quantification of affect, duration & downtime, critical services affected, geographic spread and economic impact.
9. **Define cyber threat categorization and impact analysis process:** Including likelihood, and business impact, based on the predicted affect on critical systems and business operations.
10. **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

11. **Define the scope of your DORA testing cadence:** That includes systems, tools, protocols, processes, and attack surfaces. Incorporate a preparedness analysis.
12. **Initiate DORA testing cadence for ICT Risk:** Conduct regular and comprehensive testing for all ICT exposure risks, across all attack surfaces.
13. **Initiate DORA testing cadence for Security Defenses:** Conduct regular and comprehensive testing for all security defenses, and threat detection solutions.
14. **Initiate DORA testing cadence for Incident Management Processes:** Conduct regular testing of ICT-related Incident Management Processes and systems and response measures.
15. **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
Managing of ICT third-party Risk

16. **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.
17. **Declare which of the above provides Critical ICT services:** Specify which third-parties deliver services deemed critical to the operation of the business.
18. **Define Oversight committee, with roles and responsibilities:** Review the requirements of the Lead Overseer for each ICT-related service provider.
19. **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.
20. **Harmonize processes and communication with partners:** Work with ICT-related service providers to continually learn and evolve risk analysis, testing, and communication processes.

CHAPTER VI
Information Sharing Arrangements

21. **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.
22. **Foster a culture of intelligence sharing:** with industry counterparts, partners, and third-party ICT-related service providers.
23. **Select qualified and reputable partners for consultative support and guidance:** Establish a bi-direction information sharing and communication flow.
24. **Stay informed and up to date with DORA requirements:** Establish a clear line of communication with regulators and authorities.
25. **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.

● Steps supported by the XM Cyber Platform ○ Steps not currently supported by XM Cyber.

CHAPTER II

ICT Risk Management

In order to maintain full control over ICT risk, financial entities need to have comprehensive capabilities to enable a strong and effective ICT risk management framework.

The Digital Operational Resilience Act ensures Financial entities shall have in place an internal governance and control framework to manage ICT risk, with an aim to achieve a high level of digital operational resilience. This framework should be documented and reviewed at regular intervals to enhance and improve its effectiveness. The management body of the financial entity is responsible for defining, approving, overseeing, and implementing this framework.

Financial entities shall have a sound, comprehensive, and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently, and comprehensively and to ensure a high level of digital operational resilience.

The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols, and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, and servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centers, and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorized access or usage.

The framework should include:

- Setting and approving the digital operational resilience strategy, that establishes clear roles and responsibilities.
- Define risk appetite and monitor risk levels stay within the tolerance level.
- Establish a reporting structure and process, with periodical reviews and ICT internal audits.
- Allocate and periodically review the budget related to DORA.
- Implement and fully document an ICT risk management framework to maintain resilient ICT systems.
- Identify, classify, and document critical or important functions and assets.
- Continuously monitor all sources of ICT risks in order to establish protection and prevention measures.
- Establish comprehensive threat detection mechanisms to promptly detect anomalous activities, deviants in security posture and expected behavior.
- Put in place dedicated and comprehensive business continuity policies and disaster and recovery plans, including yearly testing of the plans, covering all supporting functions.
- Establish mechanisms to learn and evolve both from external events as well as the entity's own ICT incidents and risk findings.

How XM Cyber Supports

CHAPTER II - ICT Risk Management

The goal of the ICT risk framework is to establish and deploy the appropriate tools, and strategies to minimize the impact of ICT risk.

As such, the XM Cyber Continuous Exposure Management Platform acts as a foundational component to deliver an ICT Risk Management Framework, by identifying security exposures across the digital attack surface, validating their exploitability using XM Attack Graph Analysis™ and prioritizing remediation efforts based on the risk they present to business-critical ICT assets and systems.

The XM Cyber platform supports the analysis and reporting of cyber security risk posture across a wide variety of ICT asset types. Utilizing a holistic approach that quantifies the exposure risk presented by vulnerabilities, misconfiguration, identity and credential issues, weak security posture, and poor cyber hygiene. These insights can be used to form a baseline of the current security posture, that factors in the risk to business-critical assets and operations. They can be leveraged to define proactive defense strategies, policies, and procedures to minimize risk and enhance digital operational resilience.

The XM Cyber platform provides the following key use cases for ICT Risk Management in DORA:

- Identification of ICT-related assets, with the discovery of their individual and specific vulnerabilities and related exposures.
- Quantification of risk using XM Attack Graph Analysis™ to establish the impact risk to critical ICT assets.
- Remediation guidance to close exposure gaps, and better protect the financial entity from cyber threats.
- Continuous attack scenario testing, to ensure remediation steps had a positive impact on risk reduction, to prevent future incidents.
- Detection of weakness in the external attack surface of the financial entity, and exposed credentials of their employees.
- Rich contextual insights into the exposure posture in ICT assets, for post-incident analysis to enhance learning and accelerate the evolution of the ICT risk management framework.

XM Cyber

Steps to Success:
ICT Risk Management

1. **Document critical ICT Assets and Business functions:** Identify Critical Assets and align them to classification groups based on criticality levels.
2. **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.
3. **Define risk appetite and tolerance levels:** Monitor detection thresholds and related processes to ensure they remain in line with desired tolerance.
4. **Implement resilience of business-critical systems:** Ensure the safety, security, availability, integrity, backup, and recovery of ICT systems and Data.
5. **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

In conjunction with a comprehensive ICT risk management framework, financial entities must also incorporate the appropriate mechanisms and policies for handling all ICT-related incidents, tracking cyber threats, and for reporting major ICT-related incidents.

DORA aims to structure and control the ICT-related incident handling to harmonize incident classification, response, and reporting processes.

Chapter III of the act outlines the need to establish, ICT-related incident reporting thresholds and reporting cadence. The improvements outlined in the article, are aimed at driving early detection of incidents and cyber threats while ensuring timely response, remediate, and recovery from incidents, all while minimizing downtime of critical ICT systems and services.

Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling, and follow-up of ICT-related incidents, to ensure that root causes are identified, documented, and addressed in order to prevent the occurrence of such incidents. Incident reporting should include, a quantification of the effect, the duration of the incident, and any resulting downtime, including the critical services affected, the geographical spread of the incident, and the economic impact to the business. In order to implement effective ICT-related Incident Management and Reporting. DORA defines several key steps to success:

- **Establish a comprehensive incident management and response strategy.**
- **Streamline the process to detect, log, and classify all ICT-related incidents**
- **Define thresholds for Incident classification levels, Minor, Major, and Critical Breach.**
- **Define cyber threat categorization and impact analysis process.**
- **Harmonize and evolve ICT Management Processes.**
- **ICT-related incident reporting thresholds and taxonomies vary significantly at a national level.**

Where a financial entity is subject to supervision by more than one national competent authority referred to in Article 46, Member States shall designate a single competent authority as the relevant competent authority responsible for carrying out the functions and duties provided for in this Article.

Where a major ICT-related incident occurs and has an impact on the financial interests of clients, financial entities shall, without undue delay as soon as they become aware of it, inform their clients about the major ICT-related incident and about the measures that have been taken to mitigate the adverse effects of such incident.

In the case of a significant cyber threat, financial entities shall, where applicable, inform their clients that are potentially affected of any appropriate protection measures which the latter may consider taking.

How XM Cyber Supports

CHAPTER III - ICT-related Incident Management, Classification, and Reporting

To align with this requirement financial entities must have suitable awareness of the root cause for major ICT-related incidents. They must also have suitable intelligence relating to the cyber threats that present a risk to business operations and confidential data.

To support these requirements the XM Cyber platform provides rich contextual information to support post-incident investigation and root cause analysis of major ICT incidents.

Contextual Insights for Incident Management, Classification, and Reporting through XM Cyber Platform provide the following advantages:

- Attack Path insights to support advanced Threat Hunting and post-incident investigation.
- Validated exposure exploitability findings for incident investigation to accelerate learning and evolution of processes.
- Minimize threat recurrence likelihood through exposure profiling, and targeted remediation.

For Incident Investigation and Reporting:

The insights provided by the platform can support the initial investigation to help identify the breach point and the attack techniques that may have been leveraged, leading to the Incident.

After the root cause has been understood, new attack scenarios can be created to model if a similar attack pattern is still possible. Grouping ICT Assets that share the same exposure profile as the breach point, the new scenario will discover all possible attack paths across the ICT infrastructure, towards the Critical Assets that were the target of the previous ICT-related Incident, to fully assess the likelihood of a similar incident occurring in the future. Steps can then be taken to remediate the exposures and prevent future incidents.

For Cyber Threats:

The XM Cyber platform provides a foundational level of exposure risk awareness, that is instrumental in the correlation between Cyber Threat likelihood and Impact Risk analysis. Through XM Attack Graph Analysis™ which identifies all security exposures and the TTPs that can exploitable those exposures, validating all possible attack paths across the ICT Infrastructure, prioritized by the number of critical assets placed at risk by the cyber threat.

These insights help financial entities quantify the potential effect of a cyber threat, including the geographical spread of an attack, and the potential impact to critical servers and systems that contain sensitive and confidential customer data.

XM Cyber

Steps to Success: ICT-related Incident Management, Classification, and Reporting

6 **Establish a comprehensive incident management and response strategy:** That encompasses technology, people, and processes for both Incidents and Cyber threats.

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

8 **Define thresholds for Incident classification levels:** Criteria to consider include, quantification of affect, duration & downtime, critical services affected, geographic spread and economic impact.

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

10 **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

Rigorous Digital operational resilience testing forms an essential step on the journey to success with the Act, and the critical component to periodically check the effectiveness of both the ICT Risk Management framework and the ICT-related Incident Management Processes, with an aim to deliver maximum operational resilience across financial systems and services.

Historically other previously developed regulatory frameworks in certain financial subsectors have struggled to address suitable measures and processes for effective testing of the underlying technology, people, and process, which has often resulted in increased operating costs, and inconsistent reporting of the results of digital operational resilience testing across the financial industry.

DORA aims to address this with a consistent and comprehensive approach to testing, in order to remedy those challenges.

DORA also introduces a new requirement for Financial Entities to work with suitability certified professionals, to conduct an advanced Threat-Led Penetration Testing (TLPT) at least once every three years.

Digital Operational Resilience Testing Categories and requirements include:

- Vulnerability assessments and scans
- Open source analyses
- Network security assessments
- Gap analyses
- Physical security reviews
- Questionnaires
- Scanning software solutions
- Source code reviews
- Scenario-based tests
- Compatibility testing
- Performance testing
- End-to-end testing
- Penetration testing

‘threat-led penetration testing (TLPT)’

means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity’s critical live production systems.

How XM Cyber Supports

CHAPTER IV - Digital Operational Resilience Testing

Continuous security testing is a fundamental principle of the XM Cyber Continuous Exposure Management platform. The platform delivers a comprehensive, continuous and automated approach to identify high-impact risks to critical ICT assets. To support the digital operational resilience testing the XM Cyber platform provides three key use cases and capabilities, for both period and continuous testing:

- Proactive Exposure Risk Analysis
- Continuous Threat-led Penetration Testing
- Critical Security Control Monitoring

XM Cyber Platform testing capabilities suitable for this chapter include:

Vulnerability Assessments
- Devices and Operating Systems
- Products, Software and Solutions

End-to-end Testing
- External Exposure Gap Analysis
- Exposed Credential Analysis
- Attack Path Modelling
- Cloud Security Posture Testing

Threat-Led Penetration Testing
- Scenario-based testing
- Breach Attack Simulation

XM Cyber for Threat-Led Penetration Testing:

In order to conduct an extensive Threat-led Penetration Test (TLPT) financial entities must incorporate a holistic "Red team" exercise, which must simulate all elements of a real cyber-attack, and test the entire attack surface.

This includes three key layers of the attack surface:

1. The Digital attack surface, of all ICT-related assets, infrastructure, systems, services, and tools.
2. The Physical attack surfaces, such as the campus, branch offices, data center facilities, head office, and other physical locations, which are vulnerable to an on-site intrusion.
3. The Human attack surface, which relates to both the employees and the customers of the financial entity, who may be targeted by attackers through social engineering, phishing, extortion, and credential theft.

The XM Cyber Platform acts as a foundational tool for Threat-led Penetration Testing of the **Digital Attack Surface.**

The XM Security Control Monitoring module for the XM Cyber platforms also supports Criticality Security Control analysis and infrastructure hardening for a broad range of security systems and tools. That can be used as part of Network Security testing.

XM Cyber

Steps to Success: Digital Operational Resilience Testing

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

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

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

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

15 **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

Managing of ICT third-party Risk

As an extension of the need for a comprehensive ICT Risk Management Framework, DORA aims to ensure that all third-party provided ICT services used within the Financial Entity undergo the same level of risk analysis, incident management, and rigorous testing.

The Digital Operational Resilience Act ensures Financial entities shall have in place both the internal governance and the oversight responsibilities for all ICT-related third-party service providers.

This chapter in the Act outlines the following drivers and requirements.

Financial entities' reliance on the use of ICT services is partly driven by their need to adapt to an emerging competitive digital global economy, to boost their business efficiency, and to meet consumer demand. The nature and extent of such reliance has been continuously evolving in recent years, driving cost reduction in financial intermediation, enabling business expansion and scalability in the deployment of financial activities while offering a wide range of ICT tools to manage complex internal processes.

The extensive use of ICT services is evidenced by complex contractual arrangements, whereby financial entities often encounter difficulties in negotiating contractual terms that are tailored to the prudential standards or other regulatory requirements to which they are subject, or otherwise in enforcing specific rights, such as access or audit rights, even when the latter are enshrined in their contractual arrangements.

Moreover, many of those contractual arrangements do not provide for sufficient safeguards allowing for the fully-fledged monitoring of subcontracting processes, thus depriving the financial entity of its ability to assess the associated risks. In addition, as ICT third-party service providers often provide standardized services to different types of clients, such contractual arrangements do not always cater adequately for the individual or specific needs of financial industry actors.

Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards.

Before entering into a contractual arrangement on the use of ICT services, financial entities shall:

- Assess whether the contractual arrangement covers the use of ICT services supporting critical systems and services.
- Identify and assess all relevant risks in relation to the contractual arrangement.
- Undertake all due diligence on prospective ICT third-party service providers, to ensure safety, security, and integrity of systems and data.

Financial entities shall report at least yearly to the competent authorities on the number of new arrangements for the use of ICT services, the categories of ICT third-party service providers, the type of contractual arrangements, and the ICT services and functions that are being provided.

How XM Cyber Supports

CHAPTER V - Managing of ICT third-party Risk

To align with this requirement financial entities should conduct thorough risk assessments of third-party ICT service providers before entering into, and during their contractual agreement for services.

To support these requirements the XM Cyber Platform provides two key use case advantages for the Management of ICT Third-party Risk:

- Simplify third-party ICT risk analysis through external exposure intelligence for potential ICT Service Providers.
- Continuous Threat Modelling for the risk presented to business-critical assets from third parties & supply chain.

Each use case helps extend the ICT Risk Management Framework and the Digital Operational Resilience Testing requirements to be inclusive of ICT third-party service providers.

External Exposure Intelligence of Potential Third-party ICT Service Providers:
The XM Attack Surface Management module and XM Exposed Credentials Modules can be used as part of a third-party assessment, providing threat intelligence of exposure risk on the ICT services providers' external attack surface. This should form part of a thorough risk assessment prior to provisioning the contractual service.

Continuous Threat Modelling for risk to business-critical assets from third-party systems:
The XM Cyber platform supports the creation of specific attack scenarios that model the risk of a breach, that may result from the compromise of the third-party ICT service provider and/or the ICT assets they provide to the financial entity.

The contextual information and insights reported can also be integrated into ICT-related Incident Management and cyber threat investigation, as well as supporting the information-sharing arrangements set out in Chapter IV.

XM Cyber

Steps to Success: Managing of ICT third-party Risk

16 **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.

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

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

19 **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.

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

CHAPTER VI

Information Sharing Arrangements

With ICT risk becoming more complex and sophisticated, good measures for the detection and prevention of ICT risk depend to a great extent on the regular sharing between financial entities of threat and vulnerability intelligence. Information sharing contributes to creating increased awareness of cyber threats. In turn, this enhances the capacity of financial entities to prevent cyber threats from becoming real ICT-related incidents and enables financial entities to more effectively contain the impact of ICT-related incidents and recover faster. In the absence of guidance at Union level, several factors seem to have inhibited such intelligence sharing, in particular uncertainty about its compatibility with data protection, anti-trust, and liability rules.

In addition, doubts about the type of information that can be shared with other market participants, or with non-supervisory authorities (such as ENISA, for analytical input, or Europol, for law enforcement purposes) lead to useful information being withheld. Therefore, the extent and quality of information sharing currently remains limited and fragmented, with relevant exchanges mostly being local (by way of national initiatives) and with no consistent Union-wide information-sharing arrangements tailored to the needs of an integrated financial system. It is therefore important to strengthen those communication channels.

Financial entities should be encouraged to exchange among themselves cyber threat information and intelligence, while they work collectively to leverage their individual knowledge and practical experience at strategic, tactical, and operational levels with a view to enhancing their capabilities to adequately assess, monitor, defend against, and respond to cyber threats, by participating in information sharing arrangements.

It is therefore necessary to enable the emergence at Union level of mechanisms for voluntary information-sharing arrangements which, when conducted in trusted environments, would help the community of the financial industry to prevent and collectively respond to cyber threats by quickly limiting the spread of ICT risk and impeding potential contagion throughout the financial channels.

Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts, and configuration tools, to the extent that such information and intelligence sharing:

- Enhances digital operational resilience.
- Takes place within trusted communities of the financial entities.
- Is conducted in a way that ensures data confidentiality and integrity.

How XM Cyber Supports

CHAPTER VI - Information Sharing Arrangements

Threat actors typically operate a very open community of information sharing to pool knowledge of attack techniques, tactics, processes, and even the best tools to use at each stage of the cyber kill chain.

As such, they often have the upper hand compared to Cybersecurity defenders and the organizations they are trying to protect. Data stored in siloed solutions and bound by restrictive controls can leave individual security teams and organizations feeling isolated and alone in their struggles to design and implement effective security controls and defensive strategies.

DORA aims to address this to foster a culture of collaboration across the financial sector.

In itself, this Chapter of DORA is focused on the People and Process side of cyber security, rather than the technology capabilities. However, there are some key factors to consider when selecting the right types of technology to use.

Historically there has been some hesitancy to adopt SaaS-based security solutions for Critical Infrastructure and services, but one advantage some SaaS-powered solutions do offer over their On-prem Siloed variants, is a "Collective Defense" methodology.

Collective Defense is typically a methodology where, although the data in each individual customer tenant is siloed and segregated, the overall trends and activities detected in the Cloud can be analyzed holistically to track anomalies and attack patterns across the entire dataset. These SaaS-powered solutions like XM Cyber, typically have a set of security research specialists on hand to further analyze these trends and refine the accuracy and effectiveness of the platform and its capabilities. This information can then be fed back into the platform at the individual tenant level as a Threat Intelligence feed.

To further enhance the Collective Defense strategy, organizations can also look for additional support at the human level through a security vendor's own in-house team of experts, or by partnering with MSSPs offering additional value-added Managed Services around the security solution.

Another key consideration when selecting the right security tools, to aid with this Chapter of DORA, is about the level of Information they actually provide. The richer the contextual information your tools can provide related to ICT Risk, and ICT-related Incidents, the easier it will be for you to understand and share with your trusted counterparts across the industry.

XM Cyber

Steps to Success: Information Sharing Arrangements

21 **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.

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

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

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

25 **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.

Conclusion and Key Takeaways

In today's fast-paced financial environment, maintaining operational resilience is crucial for success. As markets, technologies, and threats evolve, financial institutions face complex challenges to uphold stability and security. The EU's Digital Operational Resilience Act (DORA) plays a key role in guiding financial organizations toward a secure and resilient future.

DORA goes beyond being a mere regulatory framework; it is a strategic necessity that shapes the future of operational resilience in the financial industry. With its comprehensive approach, DORA tackles the diverse challenges financial organizations encounter daily, in the face of advanced persistent threats and a dynamic competitive landscape.

To successfully adopt DORA, is no simple task, and requires the synergy between technology, people, and processes that extends to third-party service providers and requires communication with governing bodies, and reputable peers across the finance sector.

Although no single service provider or cyber security vendor can fully deliver every article requirement across the 5 pillars of DORA, the XM Cyber Continuous Exposure Management Platform aims to deliver value to financial entities on every step of the journey.

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.

This exposure risk intelligence and rich contextual information can be utilized for incident investigation, threat hunting, and the learning and evolution of the ICT-related Incident Management processes.

The Platform provides External Attack Surface awareness and Exposed Credential threat intelligence to aid with the analysis of third-party ICT Service Providers' risk, and breach attack simulation for assessing the risk to business-critical assets present by compromised third-party assets and infrastructure.

The XM Cyber Platform can also be used to conduct a wide variety of digital operational resilience testing, from vulnerability management, through to continuous Threat-Led Penetration Testing (TLPT) of the Digital Attack Surface. We also recommend that authorized and certified specialists be consulted for holistic TLPT that combines the capabilities and findings from the XM Cyber platform with other sources of intelligence and DORA testing of both the physical and human attack surface.

Effective exposure management is crucial for financial institutions aiming to align with the Digital Operational Resilience Act. Supporting Risk Management and Incident Management with the XM Attack Graph Analysis™ to identify, prioritize and validate the exploitability of exposure across the hybrid attack surface, 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.

Detailed Matrix:

The details provided in this Matrix are for guidance purposes only in relation to implementing the Digital Operational Resilience Act.
For full details of the Articles relating to the framework please refer to: https://www.digital-operational-resilience-act.com/DORA_Articles.html
The recommendations provided in the XM Cyber Coverage column, are for guidance purposes only, and should be implement with guidance from a DORA certified professional.

CHAPTER II, ICT RISK MANAGEMENT

SECTION & ARTICLE	SUMMARY	XM CYBER COVERAGE
Article 5 **Governance and organization**	Financial entities shall have in place an internal governance and control framework to manage ICT risk, with an aim to achieve a high level of digital operation resilience. This framework should be documented and reviewed at regular intervals to enhance and improve it's effectiveness. The management body of the financial entity are responsible for defining, approving, overseeing, and implementing this framework. The framework should include: • Establish clear roles and responsibilities. • Setting and approving the digital operational resilience strategy.• Define risk appetite and monitor tolerance level. • Review periodical ICT internal audits. • Allocate and periodically review budget related to budget. • Establish a reporting structure and process. • Implement an ICT risk management framework from Article 6.	
Article 6 **ICT risk management framework**	Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently, and comprehensively and to ensure a high level of digital operational resilience. The ICT risk management framework shall include at least strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centers and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorized access or usage.	The goal of the ICT risk framework is to establish and deploy the appropriate tools, and strategies to minimize the impact of ICT risk. The XM Cyber platform supports the analysis and reporting of cyber security risk posture across a wide variety of ICT asset types. With a focus on Continuous Exposure Management, the insights and analysis provided by the XM Cyber platform focuses on the Risk presented by vulnerabilities, misconfiguration, identity and credential issues, weak security posture and poor cyber hygiene. These insights can be used to form a baseline of the current security posture, that factors in the risk to business-critical assets and operations. They can be leveraged to define proactive defense strategies, policies and procedures to minimize risk, and enhance digital operation resilience.
Article 7 **ICT Systems, protocols, and tools**	In order to address and manage ICT risk, financial entities shall use and maintain updated ICT systems, protocols and tools that are appropriate to the magnitude of operations supporting the conduct of their activities.	The XM Cyber platform provides in-depth ICT asset profile data regarding current system state and configuration. These ICT asset attributes are used to determine weakness in the attack surface, poor cyber hygiene and misconfigurations that present a risk to the business. This includes Identifying: • Legacy and unsupported ICT systems • Insecure protocol use. • Missing and misconfigured security agents and tools. • Misconfigured and non-compliant security and infrastructure tools. • Monitoring of Critical Security Control to ensure they remain in tolerance.

CHAPTER II, ICT RISK MANAGEMENT

SECTION & ARTICLE	SUMMARY	XM CYBER COVERAGE
Article 8 **Identification**	As part of the ICT risk management framework referred to in Article 6(1), financial entities shall identify, classify and adequately document all ICT supported business functions, roles and responsibilities, the information assets and ICT assets supporting those functions, and their roles and dependencies in relation to ICT risk. Financial entities shall, on a continuous basis, identify all sources of ICT risk, in particular the risk exposure to and from other financial entities, and assess cyber threats and ICT vulnerabilities relevant to their ICT supported business functions, information assets and ICT assets. Financial entities shall review on a regular basis, and at least yearly, the risk scenarios impacting them.	The XM Cyber platform will discover ICT assets, across all network locations and environments from Public cloud to On-Premises, Physical to virtual devices and user entity types, including credentials, API tokens and security groups. Each ICT Asset will be assessed for the individual exposure risk they pose to the business, prioritized based on risk to business-critical assets. The Platform has fully customizable Attack Scenarios that are utilized to analyze the risk of cyber threats, vulnerabilities and other exposure types. Each Scenario can be run periodically at a frequency suitable to the financial entities risk appetite for the given scenario, with a XM Security Posture score calculated and reported for each iteration of the scenario. These scores can be used to track risk over time, to help customers improve their security posture and digital resilience. Specific Scenarios have be tailored to assess the exposure risk of third-party service provides and can be integrated with external attack surface threat intelligence.
Article 9 **Protection and Prevention**	For the purposes of adequately protecting ICT systems and with a view to organizing response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimize the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures, to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data. Develop and document an information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customer. Scope of requirement includes: • Strong Authentication Methods • Establish a least privilege methodology to limit physical & logic access to ICT assets. • ICT Change Management, for software, hardware, firmware and security parameters. • Documented policies and procedures for patches and update Following a risk-based approach, to establish a sound network and infrastructure management structure using appropriate techniques, methods and protocols that may include implementing automated mechanisms to isolate affected information assets in the event of cyber-attacks. Financial entities shall design the network connection infrastructure in a way that allows it to be instantaneously severed or segmented in order to minimize and prevent contagion, especially for interconnected financial processes.	Although not predominately focused on data confidentially, the XM Cyber platforms delivers four key use cases to support Article 9: 1. Security Control Monitoring for Data Leakage Prevention (DLP) solutions. 2. Identity security services to support a least privilege access methodology. 3. Analysis of, and recommended guidance for patches and updates to minimize risk. 4. Testing of and recommendations for network segmentation to limit the blast radius of a cyber threat. The XM Security Control Monitoring module for the XM Cyber platforms supports integrations with a variety of DLP solutions, Identity and Authentication systems, and Network Infrastructure components, which can help to ensure the availability and integrity of suitable controls, such as cryptographic services, to an aim to protect confidentiality of data. Although the module doesn't specific provide the required functionality of each of these services, it continuously monitoring each of the security tools and systems to ensure they are operating correctly and within the predefined thresholds as part of the ICT Risk management framework. The XM Cyber platform can help discover identity and credentials issues, such as locally cached domain credentials, over-privileged user accounts, inactive user accounts and security groups, as well as externally exposed and leaked credentials. The insights provided by the platform can help customers remove unnecessary access rights, and over-privileged accounts in both on-prem and cloud infrastructure to support a least privilege access methodology, for Critical ICT assets and systems. The attack scenarios help customer zero in on outdated operating systems, and unpatched ICT assets, and provide recommendations for remediation actions through guided playbooks. To help ensure systems are kept up to date and in line with the patching strategy. The remediation guidance provided by the XM Cyber platform includes best practices for network segmentation and other infrastructure hardening steps.
Article 10 **Detection**	Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17, including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure. All of which shall be regularly tested in accordance with Article 25. Theses detection mechanisms must: • Enable multiple layers of control. • Define alert thresholds. • Trigger and initiate ICT-related incident response processes, including automatic alert mechanisms for relevant staff in charge of ICT-related incident response.	Although not predominately focused on threat detection, the XM Cyber platforms delivers two key use cases to support Article 10: • Anomaly detection and divergence of Critical Security Controls. • Trigger & initiate incident response processes as a result of high-risk divergence of security posture. After establishing the required Critical Security Controls (CSCs) for each Security tools and system, the XM Security Controls Monitoring modules can monitor and alert on divergence from the baseline and configuration drift. Thresholds for configuration drift and CSC anomaly detection can be set based on the risk appetite of the financial entity. The XM Cyber platform can also trigger alerts, either automatically through email notification or through a ICT Ticket creation process for any changes related to the XM Security Posture Score, where an anomaly is the detected in any attack scenario resulting in a change to the Risk score, or a divergence in the number of critical assets at risk, in the given scenario, that may have resulted from a cyber-attack, or configuration change resulting in an increase in exposure risk of the financial entity.

CHAPTER II, ICT RISK MANAGEMENT

SECTION & ARTICLE	SUMMARY	XM CYBER COVERAGE
Article 11 **Response and Recovery**	Financial entities shall put in place a comprehensive ICT business continuity policy, which may be adopted as a dedicated specific policy, forming an integral part of the overall business continuity policy of the financial entity. For more details on the requirement see: https://www.digital-operational-resilience-act.com/Article_11.html	Although not directly applicable to the requirements of Article 11. The XM Cyber Platform can support post-incident investigation and analysis, that can be used to help understand how a breach occurred, and what steps could be taken to minimize the chance of recurrence of the incident.
Article 12 **Backup policies and recovery methods**	For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document: • Backup policies and procedures • Restoration and recovery procedures	Not applicable to the capabilities of the XM Cyber Platform.
Article 13 **Learning and evolving**	Financial entities shall have in place capabilities and staff to gather information on vulnerabilities and cyber threats, ICT-related incidents, in particular cyber-attacks, and analyze the impact they are likely to have on their digital operational resilience. Financial entities shall put in place post ICT-related incident reviews after a major ICT-related incident disrupts their core activities, analyzing the causes of disruption and identifying required improvements to the ICT operations.	The XM Cyber platform acts as a key source of post-incident analysis to support the learning and evolution of the ICT Risk Management framework and processes. The platform provides rich contextual information regarding vulnerabilities, misconfigurations, and other exposure types, along with detailed reporting of the attack techniques that validate the exploitability of each ICT asset, along attack paths to critical assets. This data can be used to enrich Security incidents in SIEM, SOAR and XDR platforms. Or to validate the possible attack paths that may have led to the breach or ICT-related disruption of services. After the analysis learning has been completed, new attack scenario's can be created to emulate the breach hypothesis and test if such a breach can be recreated, in the recovered infrastructure.
Article 14 **Communication**	Financial entities shall have in place crisis communication plans enabling a responsible disclosure of, at least, major ICT-related incidents or vulnerabilities to clients and counterparts as well as to the public, as appropriate.	Not applicable to the capabilities of the XM Cyber Platform.
Article 15 **Further harmonization of ICT risk management tools, methods, processes and policies**	This article explains the process for the further evolution and development of technical standards relating to the ICT Risk Management Framework for DORA. For further information see: https://www.digital-operational-resilience-act.com/Article_15.html	
Article 16 **Simplified ICT risk management framework**	This article outlines the amendments to DORA for small and non-interconnected investment firms, payment institutions exempted pursuant to Directive (EU) 2015/2366. For further information see: https://www.digital-operational-resilience-act.com/Article_16.html	

CHAPTER III, ICT-RELATED INCIDENTS MANAGEMENT, CLASSIFICATION and REPORTING

SECTION & ARTICLE	SUMMARY	XM CYBER COVERAGE
Article 17 **ICT-related incident management process**	Establish and implement an ICT-related incident management process to detect, manage and notify ICT-related incidents. Financial entities shall record all ICT-related incidents and significant cyber threats. Financial entities shall establish appropriate procedures and processes to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents, to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.	To align with this requirement financial entities must have suitable awareness on the root cause for major ICT-related incidents. They must also have suitable intelligence relating to the cyber threats that present a risk to business operations and confidential data. To support these requirements the XM Cyber platform provides rich contextual information to support post-incident investigation and root cause analysis of major ICT-Incidents. **For Incident Investigation and Reporting:** The insights provided by the platform can support the initial investigation to help identify the breach point and the attack techniques that may have been leveraged, leading to the Incident. After the root cause has been understood, new attack scenarios can be create to model if a similar attack pattern is still possible. Grouping ICT Assets that share the same exposure profile as the breach point, the new scenario will discover all possible attack paths across the ICT infrastructure, towards the Critical Assets that were the target of the previous ICT-related Incident, to fully assess the likelihood of a similar incident occurring in the future. Steps can then be taken to remediate the exposures and prevent future incidents. **For Cyber Threats:** The XM Cyber platform provides a foundational level of exposure risk awareness, that is instrumental in the correlation between Cyber Threat likelihood and Impact Risk analysis. Through XM Attack Graph Analysis™ which identifies all security exposures and the TTPs that can exploitable those exposures, validating all possible attack path across the ICT Infrastructure, prioritized by the number of critical assets placed at risk by the cyber threat. These insights help financial entities quantify the potential affect of a cyber threat, including geographical spread of an attack, and the potential impact to critical servers and systems that contain sensitive and confidential customer data.
Article 18 **Classification of ICT-related incidents and cyber threats**	Financial entities shall classify ICT-related incidents and shall determine their impact based on the following criteria: • Quantification of affect • Duration of incident of downtime • Geographical spread (EU Member states) • Confidential Data Loss • Criticality of services affected. • Economic Impact Financial entities shall classify cyber threats as significant based on the criticality of the services at risk, including the financial entity's transactions and operations, number and/or relevance of clients or financial counterparts targeted and the geographical spread of the areas at risk.	
Article 19 **Reporting of major ICT-related incidents and voluntary notification of significant cyber threats**	This article explains the process and requirements for reporting major ICT-related incidents to the relevant competent authority as referred to in Article 46. For further information see: https://www.digital-operational-resilience-act.com/Article_19.html	
Article 20 **Harmonization of reporting content and templates**	This article explains the process for the further evolution and development of technical standards relating to the ICT Incident Reporting for DORA. For further information see: https://www.digital-operational-resilience-act.com/Article_20.html	
Article 21 **Centralization of reporting of major ICT-related incidents**	This article explains the process for the further evolution and development of technical standards relating to the ICT Incident Reporting for DORA. For further information see: https://www.digital-operational-resilience-act.com/Article_21.html	
Article 22 **Supervisory feedback**	This article discusses the feedback process for the supervisory state in relation to national law, by the CSIRTs under Directive (EU) 2022/2555. With regard to the ICT Incident Reporting for DORA. For further information see: https://www.digital-operational-resilience-act.com/Article_22.html	
Article 23 **Operational or security payment-related incidents**	The requirements laid down in this Chapter shall also apply to operational or security payment-related incidents and to major operational or security payment-related incidents, where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.	

CHAPTER IV, DIGITAL OPERATIONAL RESILIENCE TESTING

SECTION & ARTICLE	SUMMARY	XM CYBER COVERAGE
Article 24 **General requirement for the performance of digital operational testing**	For the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, financial entities shall, establish, maintain and review a sound and comprehensive digital operational resilience testing program as an integral part of the ICT risk-management framework referred to in Article 6. The digital operational resilience testing program shall include a range of assessments, tests, methodologies, practices and tools.	Continuous security testing is a fundamental principle of the XM Cyber Continuous Exposure Management platform. The platform delivers a comprehensive, continuous and automated approach to identify high-impact risks to critical ICT assets. To support the digital operational resilience testing the XM Cyber platform provide three key use cases and capabilities: • Proactive Exposure Risk Analysis • Continuous Threat-led Penetration Testing • Critical Security Control Monitoring
Article 25 **Testing of ICT tools and systems**	Financial entities are required to execute appropriate and regular testing: • Vulnerability assessments and scans • Open-source analyses. • Network security assessments. • Gap analyses. • Physical security reviews. • Questionnaires. • Scanning software solutions. • Source code reviews. • Scenario-based tests. • Compatibility testing. • Performance testing. • End-to-end testing. • Penetration testing.	The XM Cyber Platform can support a broad range of digital operational resilience testing, on both a periodic and continuous basis. The testing requirements suitable for this chapter include: **Vulnerability Assessments** • Devices and Operating Systems • Products, Software and Solutions **End-to-end Testing** • External Exposure Gap Analysis • Exposed Credential Analysis • Attack Path Modelling • Cloud Security Posture Testing **Threat Led Penetration Testing** • Scenario-based testing • Breach Attack Simulation The XM Security Control Monitoring module for the XM Cyber platforms also support Criticality Security Control analysis and infrastructure hardening for a board range of security systems and tools. That can be used as part of Network Security testing.
Article 26 **Advanced testing of ICT tools, systems and processes based on threat led penetration testing (TLPT)**	Financial Entities should conduct an advanced TLPT at least once every three years. 'threat-led penetration testing (TLPT)' means a framework that mimics the tactics, techniques and procedures of real-life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems.	In order to conduct an extensive Threat-led Penetration Test (TLPT) financial entities must incorporate a holistic "Red team" exercise, which must simulate all elements of a real cyber attack , and test the entire attack surface. This includes three key layers of attack surface: The Digital attack surface, of all ICT-related assets, infrastructure, systems, services, and tools. The Physical attack surface, such as the campus, branch offices, data center facilities, head office, and other physical locations, which are vulnerable to an on-site intrusion. The Human attack surface, which relates to both the employees and the customers of the financial entity, who may be targeted by attacker through social engineering, phishing, extortion, and credential theft. The XM Cyber Platform acts a foundational tool for Threat-led Penetration Testing of the Digital Attack Surface.
Article 27 **Requirements for testers for carrying out of TLPT**	This article discusses the requirements for using certified testers to conduct Threat-led Penetration Testing for DORA. For further information see: https://www.digital-operational-resilience-act.com/Article_27.html	

CHAPTER V, MANAGING OF ICT THIRD-PARTY RISK

SECTION I, Key principles for a sound management of ICT third party risk

SECTION & ARTICLE	SUMMARY	XM CYBER COVERAGE
Article 28 **General Principles**	Financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework as referred to in Article 6. This includes any third party that provides ICT Services that run business operations of the financial entity. Requirements include: • Maintaining a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers. • Report amendments to, or the procurement of new ICT services providers on a yearly basis. • Ensure the third-party meets appropriate security standards. • Conduct a risk assessment of the use of the third-party services. • Develop an exit strategy, that ensures operational resilience in response to a failure or significant breach of the third-party	To align with this requirement financial entities should conduct thorough risk assessments of third-party ICT service providers before entering in to, and during their contractual agreement for services. To support these requirements the XM Cyber platform provides two key use cases for third-party risk management: External Exposure Intelligence of potential third-party ICT Service Providers. Continuous Threat Modelling for risk to business-critical assets from compromised third-party systems. The XM Attack Surface Management module, and XM Exposed Credentials Modules can be used as part of a third-party assessment, providing threat intelligence of exposure risk on the ICT services provides external attack surface. This should form part of a thorough risk assessment prior to provisioning the contractual service. The XM Cyber platform supports the creation of specific attack scenarios that model the risk of a breach, that may result from the compromise of the third-party ICT service Provider and/or the ICT assets they provide to the financial entity.
Article 29 **Preliminary assessment of ICT concentrations risk at entity level**		
Article 30 **Key contractual provisions**	The rights and obligations of the financial entity and of the ICT third-party service provider shall be clearly allocated and set out in writing. The full contract shall include the service level agreements and be documented in one written document which shall be available to the parties on paper, or in a document with another downloadable, durable, and accessible format. For further information see: https://www.digital-operational-resilience-act.com/Article_30.html	

CHAPTER V, MANAGING OF ICT THIRD-PARTY RISK

SECTION II, Oversight framework of critical ICT third-party service providers.

SECTION & ARTICLE	SUMMARY
Article 31 **General Principles**	ICT third-party service providers that are critical to the delivery of the business operations, systems and services for financial entities, should be deemed as "critical ICT third-party service provider' encompassing all ICT third-party service provider designated as critical in accordance with Article 31. For further information see: https://www.digital-operational-resilience-act.com/Article_31.html

CHAPTER V, MANAGING OF ICT THIRD-PARTY RISK

SECTION II, Oversight framework of critical ICT third-party service providers.

SECTION & ARTICLE
Articles 32 through to 44, explain the requirements and processes to establish an oversight framework for the ongoing management and operations of critical ICT third-party service providers. Key elements of the Oversight framework include: • Establish an Oversight forum to support the work of the Joint Committee. • Allocation of Lead Observers for each critical ICT service provider. • Understand the tasks of the Lead Overseer, their powers, and how to exercise them. • How to request information and conduct general investigations and inspections. • How to harmonize and improve processes, including international communication. **For further details please refer to the articles below:**

Article 33 https://www.digital-operational-resilience-act.com/Article_33.html Tasks of the Lead Overseer	**Article 39** https://www.digital-operational-resilience-act.com/Article_39.html Inspections
Article 34 https://www.digital-operational-resilience-act.com/Article_34.html Operational coordination between Lead Overseers	**Article 40** https://www.digital-operational-resilience-act.com/Article_40.html Ongoing Oversight
Article 35 https://www.digital-operational-resilience-act.com/Article_35.html Powers of Lead Overseer	**Article 41** https://www.digital-operational-resilience-act.com/Article_41.html Harmonization of conditions enabling the conduct of the oversight activities
Article 36 https://www.digital-operational-resilience-act.com/Article_36.html Exercise of the powers of the Lead Overseer outside the Union	**Article 42** https://www.digital-operational-resilience-act.com/Article_42.html Follow-up by competent authorities
Article 37 https://www.digital-operational-resilience-act.com/Article_37.html Request for information	**Article 43** https://www.digital-operational-resilience-act.com/Article_43.html Oversight fees
Article 38 https://www.digital-operational-resilience-act.com/Article_38.html General investigations	**Article 44** https://www.digital-operational-resilience-act.com/Article_44.html International cooperation

CHAPTER VI, INFORMATION SHARING ARRANGEMENTS

SECTION & ARTICLE	SUMMARY
Article 45 **Information-sharing arrangements on cyber threat information and intelligence**	Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing: • Enhances digital operational resilience. • Takes place within trusted communities of the financial entities. • Is conducted in a way that ensure data confidentiality and integrity. For further information see: https://www.digital-operational-resilience-act.com/Article_45.html

Stop wasting time on fixes that don't impact risk

XM Cyber gives you the context you need to make faster and more confident decisions about your security posture. Understand what critical security controls you have in place and how they are helping you align with best practices and regulatory compliance frameworks.

Now you can achieve continuous compliance across your dynamic Infrastructure, helping you reduce operational overhead and more effectively align cybersecurity technology, people, and processes to remediate misconfigurations and implement proactive critical security controls.

The platform enables you to report compliance risk, by first understanding and then validating your security risk posture and its alignment to common compliance and regulatory frameworks. Which in turn minimizes the attackers' ability to evade your security defenses and increases your overall security posture.

It's time to change how you work, by ensuring your IT and Security Operations teams have the guidance they need to design and optimize effective critical security controls, while also mobilizing effective remediation strategies, helping your
Fix Less. Prevent More.

XM Cyber