DigitalXRAID
CYBER SECURITY EXPERTS

Leveraging ISO 27001 and NIST to Meet DORA Requirements

Roadmap to DORA

The Digital Operational Resilience Act (DORA) marks a significant advancement in the regulatory landscape for financial services institutions. Crafted to bolster the resilience of the financial sector against a myriad of IT and security risks, DORA sets a precedent for stringent cybersecurity mandates. This incoming regulation encompasses a broad spectrum of digital operations, demanding a unified approach to cybersecurity, risk management, and operational continuity.

In today's digital age, the importance of robust cybersecurity measures cannot be overstated. Cyber threats are becoming more sophisticated, frequent, and damaging, posing a serious risk to the stability and trustworthiness of financial systems. DORA addresses these challenges head-on, mandating that the Board and senior management take more direct accountability for cybersecurity protections. This shift underscores a broader trend where cybersecurity is no longer viewed as a purely technical domain but as a critical component of corporate governance and strategic planning.

The scope of DORA extends deep into the operational fabric of financial institutions, affecting not just the direct operations but also their third-party affiliations, including technology providers and cloud services. The Act's comprehensive approach means that institutions must evaluate every facet of their ICT operations, from data handling and system availability, to incident reporting and recovery mechanisms.

The implications of falling short of DORA's requirements are severe. Non-compliance could lead to substantial financial penalties, reputational damage, and in extreme cases, the revocation of operating licenses. Therefore, the stakes are incredibly high, making compliance a top priority for every financial entity operating within or in connection with the EU market.

For institutions already on the path to cybersecurity excellence, aligning with the NIST Cybersecurity Framework or working towards ISO 27001:2022 certification, the journey toward DORA compliance may be less arduous. These frameworks provide a solid foundation of cybersecurity practices that dovetail with many of DORA's requirements. For instance, the risk management and control processes central to ISO 27001 can be instrumental in meeting DORA's governance demands. Similarly, the NIST framework's emphasis on identifying, protecting, detecting, responding, and recovering from cybersecurity events aligns closely with DORA's operational resilience objectives.

By leveraging existing alignments with these recognised standards, financial institutions can not only expedite their compliance efforts but also enhance their overall security posture. This guide delves into how the strategic integration of ISO 27001 and NIST standards can serve as a stepping stone to achieving DORA compliance, setting the stage for a comprehensive compliance roadmap that financial services can adopt and adapt to their specific operational contexts.

Understanding DORA, ISO 27001:2022, and the NIST Framework

DORA Overview

The Digital Operational Resilience Act (DORA) represents a crucial evolution in regulatory frameworks designed to enhance the resilience of the financial sector against a backdrop of increasing cyber threats.

This regulation mandates that financial entities within the EU, and those substantially operating or servicing European markets, establish robust mechanisms to manage and mitigate ICT risks. DORA's overarching goal is to ensure that the financial sector can withstand, respond to, and recover from ICT-related disruptions and threats.

Key Objectives and Requirements

DORA outlines five key pillars to ensure the operational resilience of financial entities. These pillars provide a framework for financial institutions to enhance their digital operational resilience and ensure compliance with regulatory standards:

Governance and Risk Management

- Requirement for robust governance structures to manage ICT risks
- Mandatory risk assessments and regular testing of ICT systems

Incident Reporting

- Obligations to establish and maintain an incident management framework
- Specific requirements for reporting major ICT-related incidents to regulatory bodies

Digital Operational Resilience Testing

- Mandates for periodic testing of ICT systems, including vulnerability assessments and penetration tests
- Requirement for critical third parties to participate in testing

ICT Third-Party Risk

- Regulations on oversight and management of third-party providers, including cloud services
- Contractual obligations to comply with DORA standards

Information and Intelligence Sharing

- Encouragement of information sharing about cyber threats and vulnerabilities within the financial sector

Compliance Deadline

The compliance deadline for DORA is set for January 2025. Financial institutions and their critical third parties must have implemented the required ICT risk management capabilities by this date.

Non-compliance can result in fines up to 1% of the daily worldwide turnover, along with reputational damages, and in severe cases, revocation of licenses.

ISO 27001:2022 Overview

ISO 27001:2022 is the latest iteration of the internationally recognised standard for an Information Security Management System (ISMS). It provides a systematic approach to managing sensitive company information so that it remains secure.

Core Elements and Structure

This standard includes components such as risk management processes, ISMS policy, objectives, internal audit, management review, continual improvement, and a set of security controls tailored to the needs of the organisation.

Significance in Establishing an ISMS

Implementing an ISMS in accordance with ISO 27001:2022 allows organisations to manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties.

It is particularly significant as it provides a structured framework to ensure the confidentiality, integrity, and availability of information.

NIST Framework Overview

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is widely acknowledged for its pragmatic and flexible approach to improving cybersecurity across industries. It is particularly valued for its ability to be tailored to the specific security needs of any organisation.

Components of the Framework

This standard includes components such as risk management processes, ISMS policy, objectives, internal audit, management review, continual improvement, and a set of security controls tailored to the needs of the organisation.

The NIST Framework is built around five core functions:

Identify

- Develop an organisational understanding to manage cybersecurity risk

Protect

- Implement appropriate safeguards

Detect

- Develop and implement appropriate activities to identify the occurrence of a cybersecurity event

Respond

- Take action on a detected cybersecurity incident

Recover

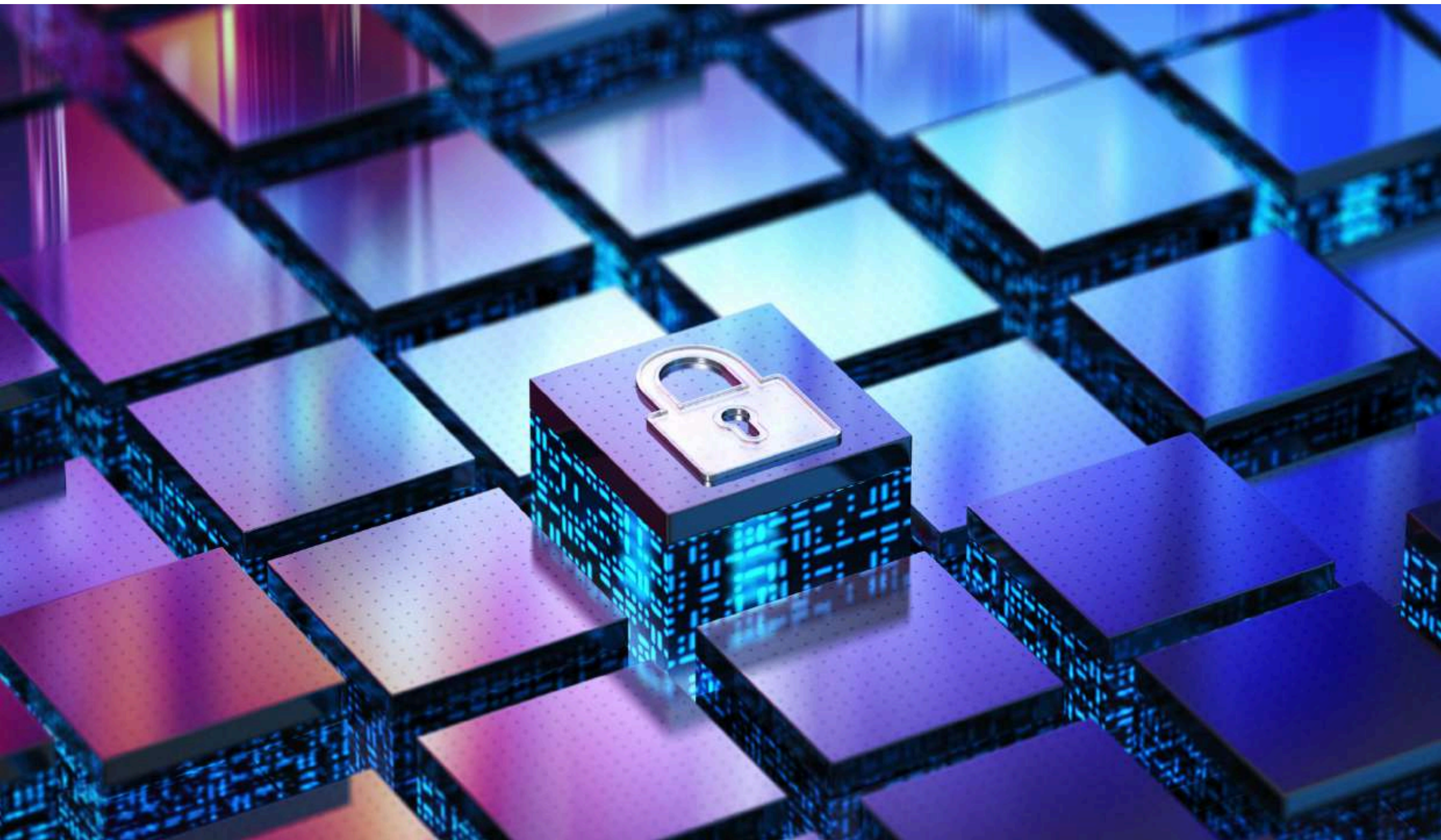
- Plan for resilience and take action to restore any capabilities or services impaired due to a cybersecurity event

Application in Improving Cybersecurity and Resilience

The application of the NIST Framework assists organisations in managing and reducing their cybersecurity risks in conjunction with other cybersecurity and governance risk management processes.

This framework is particularly helpful for organisations aiming to align their cybersecurity strategy with broader organisational needs and risk strategies.

Together, DORA, ISO 27001:2022, and the NIST Framework provide a robust set of guidelines and best practices that can significantly aid financial institutions in reinforcing their cybersecurity and operational resilience. Understanding these frameworks in depth provides a foundation for establishing a comprehensive approach to compliance and security management.



DORA, ISO 27001:2022, and NIST:

Mapping DORA Requirements to ISO 27001:2022 and NIST

To ensure compliance and enhance operational resilience, it's essential to understand how existing standards like ISO 27001:2022 and the NIST Cybersecurity Framework align with the new DORA regulations. Both frameworks offer a robust foundation that can be leveraged to meet the stringent demands of DORA, providing a structured pathway to compliance.

How ISO 27001:2022 Addresses DORA's Cybersecurity Requirements

ISO 27001:2022's comprehensive set of controls and its overarching management processes align well with DORA's requirements, particularly in areas such as risk assessment, incident management, and information security:

- **Risk Management:**

ISO 27001:2022 requires organisations to conduct thorough risk assessments, aligning with DORA's emphasis on risk management for ICT-related threats.

- **Incident Management:**

The standard's incident management requirements correlate with DORA's mandates for effective and rapid response to ICT disruptions.

- **Information Security Policies:**

These are integral to ISO 27001 and support DORA's requirement for robust governance and policies to safeguard digital operations.

DORA, ISO 27001:2022, and NIST:

Alignment of NIST Framework with DORA Mandates

The NIST Framework's core functions—Identify, Protect, Detect, Respond, and Recover—mirror the lifecycle approach that DORA advocates for managing ICT risks:

- **Identify and Protect:**

These functions help institutions map their resources and protect their infrastructure, aligning with DORA's focus on resilience against ICT risks.

- **Detect, Respond, and Recover:**

These capabilities are crucial for complying with DORA's requirements for incident response, recovery planning, and resilience, ensuring that organisations can quickly restore services following an ICT disruption.

Key Overlaps and Gaps

Detailed Comparison of Specific Clauses and Controls

- **Governance and Strategy:**

Both ISO 27001 and NIST emphasise the importance of governance, aligning with DORA's requirements for strategic management of ICT risks. However, DORA goes further by specifying the need for detailed operational resilience capabilities.

- **Third-Party Management:**

ISO 27001 includes controls for managing third-party risks which support DORA's requirements. NIST also addresses third-party risks in its Protect function, though DORA provides more detailed protocols for financial services.

- **Testing and Audits:**

DORA's requirements for rigorous testing and continuous audits are partially covered by ISO 27001's evaluation requirements and NIST's continuous monitoring suggestions.

Identifying Areas of Strong Alignment and Potential Gaps in Coverage

- **Strong Alignment:**

The strong governance and risk management focus in ISO 27001 and NIST aligns closely with DORA's strategic approach to ICT risk management.

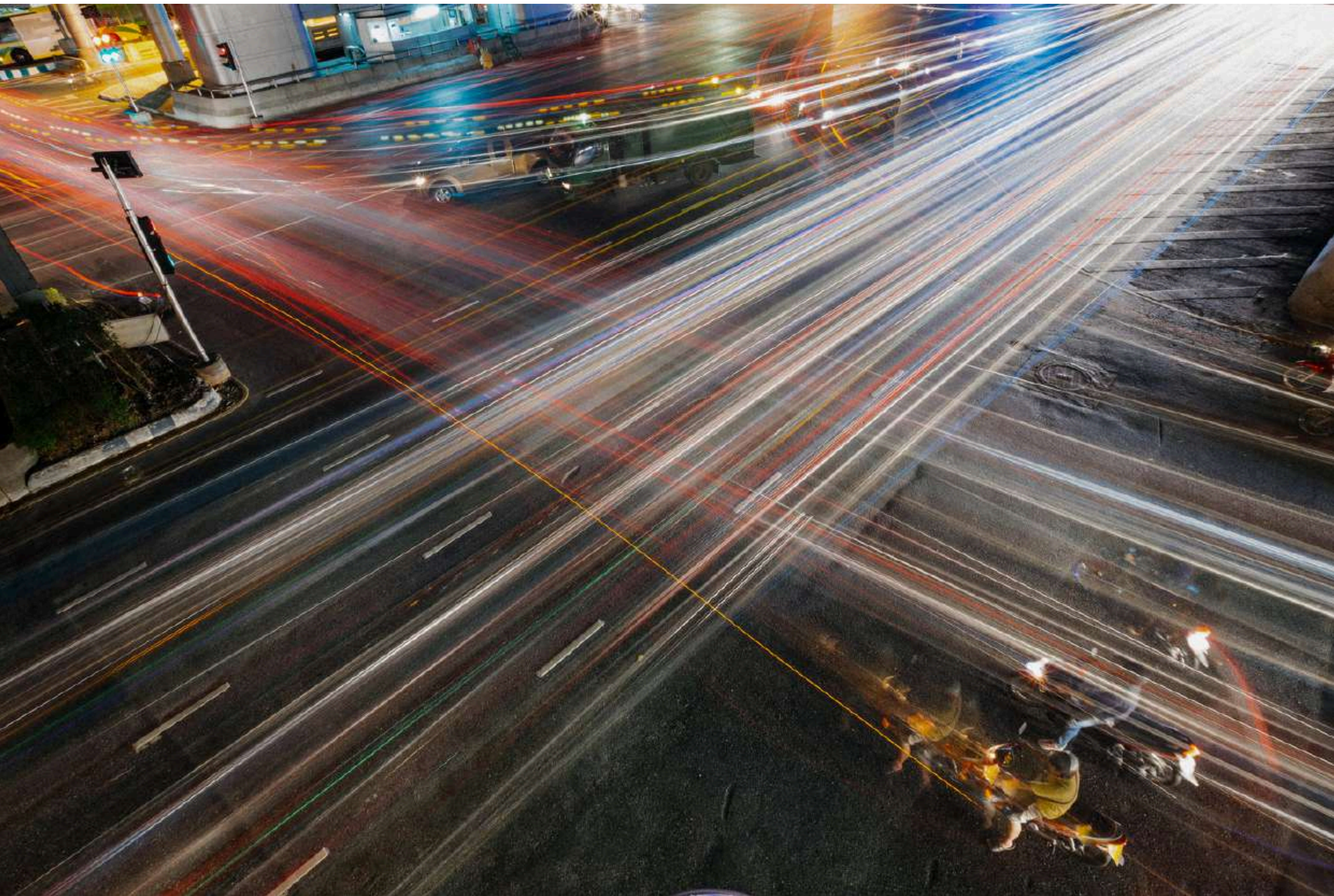
- **Potential Gaps:**

Specific areas such as extensive incident reporting mechanisms and detailed third-party controls in DORA may not be fully addressed by ISO 27001 or NIST. These areas might require additional policies or enhancements to existing practices to achieve full compliance.

The intersection of DORA with ISO 27001:2022 and the NIST Framework demonstrates significant compatibility, especially in establishing a cybersecurity baseline and governance structure.

However, the detailed demands of DORA may necessitate that financial institutions further refine their approaches, particularly in areas like third-party management and specific compliance reporting mechanisms.

This comparative analysis not only highlights the synergies but also directs attention to areas requiring augmentation to meet the comprehensive demands of DORA.



Gap Analysis and Compliance Roadmap:

Conducting a Gap Analysis with a Cybersecurity Specialist

The journey towards DORA compliance is punctuated by the need for a meticulous gap analysis, particularly where existing frameworks such as ISO 27001:2022 and NIST are already in use. Engaging a cybersecurity specialist to conduct this analysis ensures a thorough and nuanced understanding of existing practices against DORA's specific requirements.

Steps to Identify and Assess Gaps in DORA Compliance Using ISO 27001:2022 and NIST

- **Documentation Review:**

Evaluate existing security policies and procedures against DORA's requirements. This includes reviewing the scope of the Information Security Management System (ISMS) as outlined by ISO 27001:2022 and the cybersecurity practices recommended by NIST.

- **Risk Assessment Alignment:**

Compare current risk assessment methodologies with those necessitated by DORA, ensuring that all ICT risks are adequately identified and managed.

- **Control Mapping:**

Map existing controls from ISO 27001:2022 and NIST to the specific controls and requirements of DORA, identifying overlaps and detecting any areas lacking coverage.

- **Incident Response Evaluation:**

Assess the current incident response and management processes to ensure they meet the rapid response and detailed reporting requirements under DORA.

- **Third-Party Risk Management:**

Scrutinise current third-party management practices for compliance with DORA's stringent third-party policies, especially in the context of operational resilience.

Role of a Cybersecurity Service Provider in Facilitating the Analysis

A cybersecurity service provider brings expertise in bridging gaps between different regulatory frameworks and internal practices. They can offer:

- Expert guidance on interpreting DORA's clauses in the context of your business operations.
- Assistance in enhancing current cybersecurity frameworks to align with DORA’s rigorous standards.
- Recommendations for integrating new tools or practices to fill identified gaps.
- Training and awareness programs to ensure that staff at all levels understand their role in compliance and operational resilience.

Developing a Compliance Roadmap
Strategic Phases to Achieve Full Compliance by January 2025

- **Immediate Initiatives (2023):**

Begin by addressing the most critical gaps identified in the gap analysis. Prioritise quick wins that align existing policies and controls with DORA’s requirements.

- **Mid-term Actions (2024):**

Implement more complex changes, such as enhancements to incident response frameworks or third-party contracts and controls. Start regular training sessions and simulations to test the effectiveness of the new measures.

- **Long-term Adjustments (2025):**

Finalise all compliance efforts, ensuring every aspect of DORA is fully integrated into daily operations. Establish ongoing monitoring and continuous improvement mechanisms to adapt to any changes in the regulatory landscape.

Recommendations for Integrating ISO and NIST Controls into DORA Compliance Strategies

- **Leverage ISO 27001's ISMS for Comprehensive Coverage:**

Utilise the structure of ISO 27001 to ensure that all aspects of DORA are covered by your ISMS, including risk management and incident response.

- **Adopt NIST's Continuous Monitoring Practices:**

Integrate NIST's approach to continuous monitoring to enhance the detection and management of ICT risks, supporting DORA's requirements for operational resilience.

- **Harmonise Incident Reporting:**

Align ISO 27001 and NIST's incident response strategies with DORA's stringent reporting requirements, ensuring rapid and effective communication with regulators.

Reporting and Stakeholder Engagement:

Communication with the Board and External Stakeholders

Effective communication with both the board and external stakeholders is pivotal in navigating the compliance landscape. It's not just about meeting regulatory requirements; it's about fostering a culture of resilience and proactive cybersecurity management within the organisation.

Crafting Clear, Concise, and Informative Compliance Reports

Compliance reports serve as a bridge between cybersecurity operations and strategic decision-making. To craft reports that resonate with both technical and non-technical stakeholders:

- **Highlight Key Information:**

Focus on critical metrics and status updates on compliance efforts, particularly how they align with DORA's requirements.

- **Use Visual Aids:**

Incorporate charts, graphs, and tables to break down complex data into digestible visuals that clarify the extent of compliance and areas needing attention.

- **Executive Summaries:**

Provide summaries that encapsulate major points for stakeholders who need a quick overview of the status without delving into technical details.

Engaging with Stakeholders Including the Financial Conduct Authority (FCA)

Engagement with regulatory bodies such as the FCA is not just a compliance formality but a strategic engagement that enhances credibility and trust. Regular updates, aligned with compliance milestones, should be communicated to the FCA to demonstrate ongoing commitment to regulatory standards and operational resilience.

Monitoring and Continuous Improvement

The cybersecurity landscape is dynamic, with emerging threats and regulatory updates necessitating continual vigilance and adaptation.

Continuous monitoring is crucial in maintaining compliance with DORA and other regulatory frameworks. Schedule frequent assessments to review and evaluate the effectiveness of implemented controls and to ensure that they are functioning as intended within the broader cybersecurity framework.

Updating and Refining Cybersecurity Practices in Response to Emerging Threats and Regulatory Changes

Staying ahead in cybersecurity means being adaptable:

- **Feedback Loops:**

Establish mechanisms for feedback from IT and cybersecurity teams to inform about practical challenges and suggest improvements and to the Board to ensure they have full visibility of the status of cyber programs and compliance status.

- **Regulatory Updates:**

Keep abreast of any updates in DORA regulations or related guidelines, incorporating changes into the cybersecurity strategy promptly.

- **Threat Intelligence:**

Invest in threat intelligence services that provide insights into emerging threats, allowing for pre-emptive adjustments to security measures.

The journey towards achieving and maintaining DORA compliance is continuous and requires a robust strategy involving gap analysis, compliance roadmaps, and effective communication with stakeholders.

The roles of established frameworks such as ISO 27001:2022 and the NIST Cybersecurity Framework in achieving DORA compliance are clear. Financial institutions must leverage every tool at their disposal, from ISO 27001:2022's risk management processes to the NIST framework's proactive security practices, to forge a path that not only meets regulatory demands but also secures the trust and confidence of their customers and stakeholders.

By implementing a comprehensive program of monitoring and continuous improvement, financial institutions can not only comply with DORA but can also enhance their overall cybersecurity posture, ensuring resilience in the face of evolving cyber threats and regulatory demands. This proactive approach not only safeguards the institution but also reinforces its credibility and reliability in the financial sector.

Appendices

Appendix A: Relevant DORA Clauses

Governance and Risk Management

- Requirement for robust governance structures to manage ICT risks
- Mandatory risk assessments and regular testing of ICT systems

Incident Reporting

- Obligations to establish and maintain an incident management framework
- Specific requirements for reporting major ICT-related incidents to regulatory bodies

Digital Operational Resilience Testing

- Mandates for periodic testing of ICT systems, including vulnerability assessments and penetration tests
- Requirement for critical third parties to participate in testing

ICT Third-Party Risk

- Regulations on oversight and management of third-party providers, including cloud services
- Contractual obligations to comply with DORA standards

Information and Intelligence Sharing

- Encouragement of information sharing about cyber threats and vulnerabilities within the financial sector

Appendix B: ISO 27001:2022 Clauses Pertinent to DORA Compliance

Leadership and Commitment (Clause 5)

- Requirement for top management to demonstrate leadership and commitment with respect to the information security management system.

Risk Assessment and Treatment (Clause 6)

- Detailed requirements for identifying risks related to the confidentiality, integrity, and availability of information and treatment of those risks.

Security Controls (Annex A)

- Specific controls around access control, cryptography, physical security, operational security, communications security, and system acquisition, development, and maintenance.

Incident Management (Clause 16)

- Specifications for establishing an effective incident management process and responding to information security incidents accordingly.

Monitoring, Measurement, Analysis, and Evaluation (Clause 9)

- Stipulations for regular assessments of information security performance and the effectiveness of the ISMS.

Appendix C: NIST Framework Components Applicable to DORA

Identify

- Asset management: Identifying and classifying information assets.
- Business environment: Understanding the organisation’s role in the supply chain.

Protect

- Access Control: Ensuring that access to assets is controlled and managed.
- Awareness and training: Educating personnel on cybersecurity risks.

Detect

- Anomalies and Events: Establishing baseline understanding and detecting unusual activities.
- Security Continuous Monitoring: Implementing continuous monitoring mechanisms.

Respond

- Response Planning: Developing and implementing incident response capabilities.
- Communications: Coordinating response activities with internal and external stakeholders.

Recover

- Recovery Planning: Developing and implementing recovery processes.
- Improvements: Incorporating lessons learned into the recovery strategies.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence
Against Cyber Threats?
Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com