Microsoft

Microsoft Product to DORA Regulation Mapping - Guide for Customers

Background of the Digital Operational Resilience Act (DORA):

The Digital Operational Resilience Act (DORA) is a regulatory framework by the European Union, aimed at fortifying the operational resilience of the financial services sector amidst the rapidly evolving landscape of Information and Communication Technology (ICT) risks. This initiative is a response to the increasing dependency on digital technologies and the consequent vulnerabilities that have emerged, posing significant risks to the stability and integrity of financial systems.

DORA articulates a set of comprehensive requirements designed to ensure that regulated entities are adequately prepared to withstand, respond to, and recover from a variety of ICT-related disruptions and threats. These requirements span across several critical areas, including the establishment of advanced ICT risk management protocols, the implementation of robust incident reporting and management systems, the conduct of thorough digital operational resilience testing, the rigorous oversight of third-party service providers, and the facilitation of secure information sharing among stakeholders.

The regulation is applicable to a broad spectrum of entities operating within the EU financial sector including but not limited to credit institutions, investment firms, insurance companies, payment institutions, and e-money institutions. DORA underscores the significance of a holistic approach to operational resilience, emphasizing the need to adopt and integrate comprehensive strategies that address the multifaceted dimensions of digital operational resilience.

Introduction:

This guide provides a mapping for Microsoft's capabilities and solutions to the requirements under DORA and an overview of how Microsoft can help regulated institutions meet those requirements.

In navigating the complex regulatory landscape introduced by DORA, Microsoft recognizes the importance of equipping our customers with the necessary tools and insights to help meet these regulatory challenges. This guide aims to explain how Microsoft's solutions and capabilities can support compliance with DORA's mandates.

1. ICT Risk Management: Microsoft 365 E5 (Microsoft Defender for M365 & Microsoft Sentinel):

ICT Risk Management stands as a cornerstone of DORA's regulatory framework, emphasizing the necessity for regulated entities to implement proactive and dynamic strategies to identify, assess, and mitigate ICT risks.

1. ICT Risk Management: Microsoft 365 E5 (Microsoft Defender for M365 & Microsoft Sentinel): cont.

In alignment with this critical requirement, Microsoft 365 E5, featuring Advanced Threat Protection (ATP) and Microsoft Sentinel, offers an unparalleled solution that embodies the essence of proactive threat detection and response.

Advanced Threat Protection (ATP): ATP leverages sophisticated AI-driven analysis and machine learning algorithms to provide real-time protection against a broad spectrum of cyber threats. This proactive defense mechanism is instrumental in identifying emerging threats, enabling regulated entities to implement preemptive measures to mitigate risk effectively.

Microsoft Sentinel: As a cloud-native SIEM (Security Information and Event Management) system, Azure Sentinel extends beyond traditional security measures to offer intelligent security analytics and threat detection capabilities. Sentinel facilitates the aggregation, analysis, and correlation of security data across the entire digital estate, providing actionable insights that empower regulated entities to swiftly respond to identified risks.

DORA Alignment: By integrating Microsoft 365 E5's Defender suite and Microsoft Sentinel into their ICT risk management framework, regulated entities can prepare for robust compliance with DORA's mandates. This integration not only enhances an entity's ability to manage and mitigate ICT risks proactively but also aligns with DORA's overarching objective to bolster the operational resilience of the financial sector.

2. Incident Reporting and Management: Microsoft Defender and Compliance Center:

In the realm of financial services, the ability to swiftly detect, report, and manage ICT-related incidents is not just a regulatory requirement but a critical operational necessity. Microsoft Defender & Compliance Center stands at the forefront of Microsoft's solutions to help address this need, offering an integrated platform that streamlines the entire incident lifecycle.

Microsoft Defender offers broad threat protection across digital estates, helping to support early detection of potential security incidents. Its advanced analytics and threat intelligence capabilities allow for rapid response and mitigation strategies, minimizing potential impacts on operations.

Compliance Center complements these capabilities by providing a centralized dashboard for incident reporting and management. It simplifies the compliance process with automated workflows for incident documentation, assessment, and reporting, helping to support adherence to DORA's stringent requirements for timely and accurate incident communication.

DORA Alignment: Utilizing Microsoft Defender & Compliance Center helps regulated entities to not only prepare for DORA's mandates for incident reporting and management but also to enhance their overall incident response strategy, enabling a state of preparedness and resilience against ICT threats.

3. Digital Operational Resilience Testing: Azure Security Center:

Digital Operational Resilience Testing is a pivotal aspect of DORA, aimed at ensuring regulated entities' digital infrastructures can withstand and recover from disruptions. Azure Security Center provides an integrated solution for conducting continuous security assessments and resilience testing.

With Azure Security Center, regulated entities can leverage advanced scanning and analysis tools to identify vulnerabilities and assess the effectiveness of their security measures. Its continuous monitoring and assessment capabilities help enable organizations to maintain an up-to-date view of their security posture, facilitating ongoing improvements and compliance with DORA's resilience testing mandates.

4. Third-party Service Providers Oversight: Microsoft Purview:

Microsoft Purview offers an extensive suite of data governance and risk management tools.

Microsoft Purview helps regulated entities to gain comprehensive visibility into their data landscape, including data held and processed by third-party providers. Its robust governance and compliance capabilities help ensure that third-party engagements are managed effectively, with rigorous adherence to data protection and privacy standards.

DORA Alignment: Implementing Microsoft Purview as part of a third-party oversight strategy assists regulated entities to prepare to comply with DORA's requirements for managing third-party risks. It helps regulated entities enforce strict data management and security protocols across its external service providers, aligning with the regulation's objectives to safeguard the financial sector's operational resilience.

5. Information Sharing: Microsoft Information Protection and Microsoft Teams as Crisis Management Tools:

In the context of DORA, securely sharing information is critical for collective cyber defense. Microsoft Information Protection helps ensure the secure management and sharing of financial data. Microsoft Teams, when integrated with Information Protection, serves as a secure collaboration platform, potentially acting as a crisis management communication tool during major incidents. This approach aligns with DORA's mandates for secure information sharing and enhances cybersecurity in the financial ecosystem.

6. Compliance and Data Protection:

Microsoft Purview and Microsoft Priva for Data Protection: Addressing DORA's data protection emphasis, Microsoft Purview provides unified data governance, helping to enable compliance with DORA's regulatory requirements. Microsoft Priva enhances privacy management and risk assessment, supporting regulated entities in maintaining data security and compliance, thus aligning with DORA's data protection mandates.

7. Integrated Compliance Management:

Compliance Manager & Microsoft 365 Compliance Center for ICT Risk Management: To manage DORA compliance complexities, the Compliance Manager and Microsoft 365 Compliance Center offer a broad regulatory compliance management suite. These tools streamline compliance workflows, provide actionable insights, and help organizations maintain operational resilience and adhere to regulatory standards.

DORA Alignment: The integration of Compliance Manager and Microsoft 365 Compliance Center with DORA's requirements offers a robust framework for managing ICT risk, enhancing the ability of organizations to meet regulatory demands and maintain a high level of operational resilience.

8. Business Continuity:

Azure Site Recovery & Microsoft 365 Syntex Backup for Business Continuity: DORA addresses business continuity and recovery. Microsoft's Azure Site Recovery and Microsoft 365 Syntex Backup support this by providing disaster recovery and data backup solutions, respectively. These offerings help regulated entities develop resilient setups and support meeting DORA's business continuity requirements.

DORA Alignment: These solutions directly support DORA's business continuity and recovery provisions. By enabling regulated entities to develop resilient operations and recover quickly from disruptions, they support compliance with DORA's requirements, enhancing the sector's overall operational resilience.

Conclusion:

Microsoft's suite of products and services, including Microsoft 365 E5, Azure Security Center, Microsoft Purview, Microsoft Priva, Compliance Manager, and Microsoft 365 Compliance Center, provides a broad and integrated solution set to support regulated entities to meet relevant requirements under DORA. Through this guide, we have underscored our commitment to supporting our customers in achieving and maintaining regulatory compliance, thereby enhancing operational resilience and security within the financial sector.

For Personalized Assistance:

At Microsoft, we are dedicated to helping regulated entities meet DORA and other applicable regulatory requirements. To achieve this, we offer personalized assistance through our experienced team of professionals who are ready to support you at every step of the way.

- Your Local Account Executive or security specialist: For tailored guidance specific to your organization's needs and to explore how Microsoft's solutions can best support your DORA compliance journey, please reach out to your local account executive. They are well-equipped to provide you with insights and solutions tailored to your unique operational context.
- Data Privacy and Security Global Black Belt: For in-depth discussions on the technological aspects of DORA compliance and to understand the broader implications for your organization within the regulatory landscape, our Global Black Belts are at your service. They can offer expert advice on aligning Microsoft's technology solutions with your strategic compliance objectives and operational resilience goals.

Microsoft

Microsoft Product to DORA Regulation Mapping - Guide for Customers

Get in touch with your Local Account Executive or reach out directly through your existing Microsoft support channels. We are here to demonstrate how Microsoft product and service can help you navigate the DORA landscape successfully.