Gigamon for Digital Operational Resilience Act (DORA)

Framework Mapping Guide

SEPTEMBER, 2024

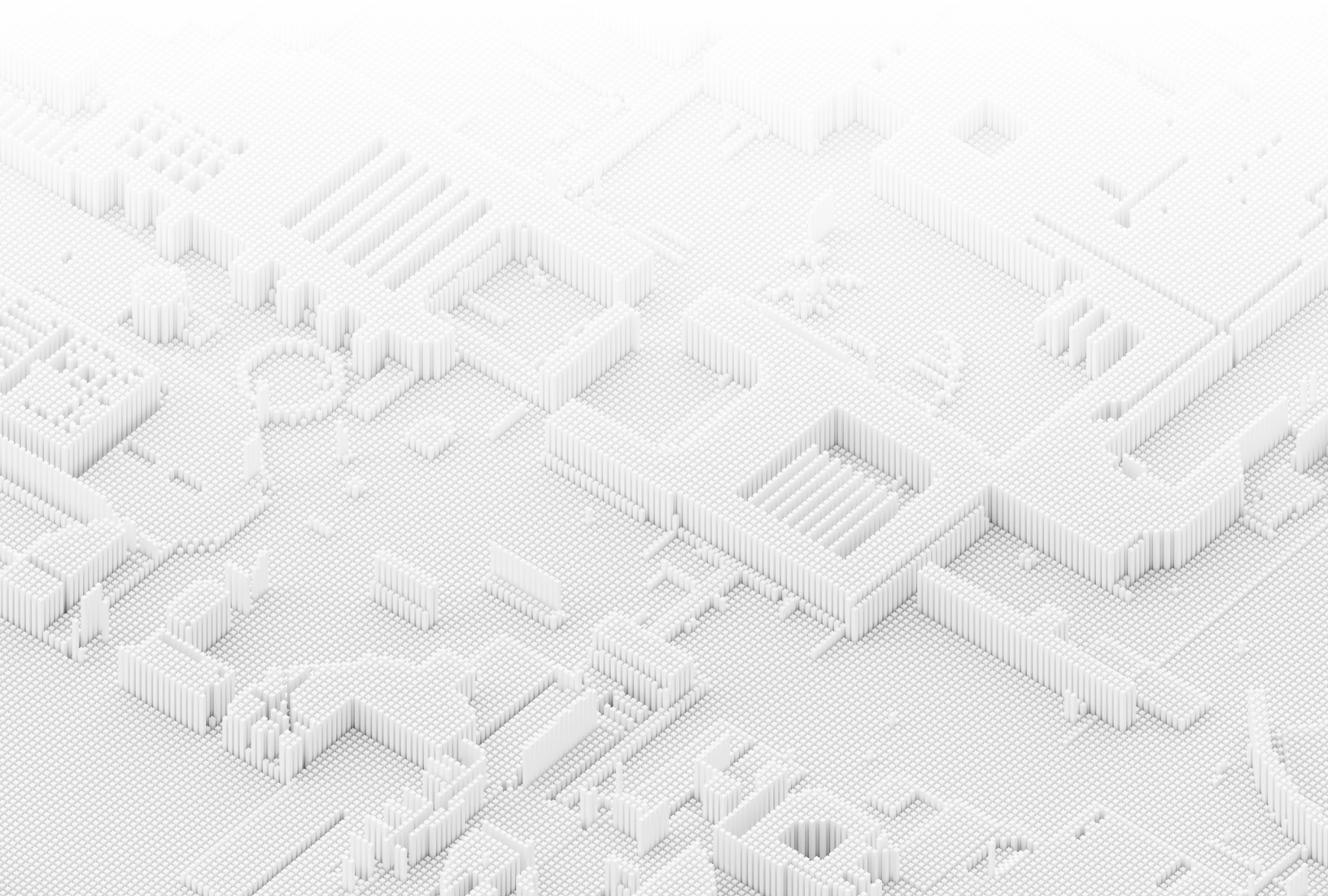

Table of Contents

Introduction

The Digital Operational Resilience Act (DORA) provides a comprehensive regulatory framework for ensuring the resilience of the EU financial sector's information and communication technology (ICT) systems. DORA outlines specific requirements for ICT risk management, incident reporting, third-party oversight, and cybersecurity resilience, with the goal of safeguarding financial institutions from ICT-related disruptions and cyber threats.

This document provides a detailed mapping of how the Gigamon Deep Observability Pipeline aligns with and supports the key requirements of DORA. By providing comprehensive visibility into all network traffic and network-derived telemetry, Gigamon empowers organisations to strengthen their operational resilience, improve incident response, and maintain compliance with DORA's rigorous standards. Gigamon plays a crucial role in enabling firms to secure their ICT infrastructure, monitor third-party risks, and enhance their overall cybersecurity posture in line with DORA's regulatory framework.

DORA and Cyber Resilience in Financial Services

In response to the growing reliance of the financial sector on digital infrastructure and the increasing risks posed by cyberattacks, technological failures, and ICT-related disruptions, there is a heightened risk that these vulnerabilities could lead to operational outages, data breaches, and significant financial instability. DORA sets out comprehensive guidelines and standards to fortify the overall security of the financial sector against potential cyber threats and disruptions that could compromise the integrity of digital operations within the EU.

DORA encompasses five main pillars (or chapters) that together ensure the resiliency of financial sector in the face of all types of Information and Communication Technology (ICT) disruptions and threats.

I: Risk Management
Requires financial institutions to implement robust frameworks for identifying, managing, and mitigating ICT risks across their operations, ensuring continuous monitoring and security.

II: Incident Reporting
Mandates timely reporting of significant ICT-related incidents to regulatory authorities, ensuring transparency and allowing for coordinated responses to cyber threats and disruptions.

III: Resilience Testing
Enforces regular testing of ICT systems, including advanced threat-led penetration tests, to evaluate their resilience against cyberattacks and operational failures.

IV: Third-Party Risk Management
Requires firms to oversee and assess the ICT risks posed by third-party service providers, ensuring that outsourced services comply with the same security and resilience standards.

V: Information Sharing
Promotes collaboration by establishing frameworks for sharing cyber threat intelligence and ICT incident information across the financial sector to enhance collective security and resilience.

Gigamon helps organisations strengthen their operational resilience, improve incident response, and maintain compliance with DORA's rigorous standards.

Pillar I

RISK MANAGEMENT

In today's evolving infrastructure landscape, where financial services institutions (FSIs) increasingly operate across hybrid and multi-cloud environments, Gigamon provides the essential visibility needed to accurately identify assets and effectively manage corporate and supply chain risks.

The Gigamon Deep Observability Pipeline enables organisations to monitor and analyse all network traffic across on-premises, virtual, and cloud infrastructure, ensuring comprehensive oversight of managed and unmanaged devices, including IT, OT, and IoT. By offering detailed insights into network behavior and vulnerabilities, Gigamon significantly reduces the risk of potential attacks, regardless of where the data resides.

Additionally, Gigamon provides network security, risk management, and extended detection and response (XDR) tools with actionable intelligence that help security teams identify threats, enforce policies, and implement effective remediation strategies, even in complex hybrid cloud environments.

Articles For Pillar I: ICT Risk Management		How Gigamon Helps
Governance and Organisation **(Article 5)**	Organisations need to create a governance framework for digital resilience, with senior management responsible for oversight. Firms must manage ICT risks, report significant incidents to authorities, and conduct regular testing to ensure their systems remain effective.	Gigamon helps organisations comply with Articles 5 and 6 of DORA by enhancing their digital operational resilience through deep observability and management of network traffic, particularly in environments where FSIs increasingly operate infrastructures that span hybrid and multi-cloud setups. Gigamon solutions enable firms to monitor and analyse data across on-premises, virtual, and cloud-based networks, ensuring effective risk management and the identification of potential threats across diverse infrastructures. This real-time deep observability supports firms in meeting DORA's requirements for ICT risk management, incident detection, and reporting, regardless of whether their data and systems are located. Additionally, Gigamon aids in the continuous testing and validation of security measures, allowing firms to maintain robust digital operational resilience across complex hybrid and multi-cloud infrastructures as required by Articles 5 and 6 of DORA.
ICT Risk Management Framework **(Article 6)**		

Articles For Pillar I: ICT Risk Management, cont'd		How Gigamon Helps
ICT Systems, protocols and tools **(Article 7)** Establish robust ICT-related incident detection and response processes, ensuring timely identification, management, and reporting of incidents to maintain digital operational resilience	**a)** Use and maintain updated ICT systems, protocols and tools that are appropriate to the magnitude of operations supporting the conduct of their activities, in accordance with the proportionality principle as referred to in Article 4.	Gigamon helps organisations comply with **Articles 5 and 6** of DORA by enhancing their digital operational resilience through deep observability and management of network traffic, particularly in environments where FSIs increasingly operate infrastructures that span hybrid and multi-cloud setups. Gigamon solutions enable firms to monitor and analyse data across on-premises, virtual, and cloud-based networks, ensuring effective risk management and the identification of potential threats across diverse infrastructures. This real-time deep observability supports firms in meeting DORA's requirements for ICT risk management, incident detection, and reporting, regardless of whether their data and systems are located. Additionally, Gigamon aids in the continuous testing and validation of security measures, allowing firms to maintain robust digital operational resilience across complex hybrid and multi-cloud infrastructures as required by **Articles 5 and 6** of DORA.
	c) Use and maintain updated ICT systems protocols and tools that are equipped with sufficient capacity to accurately process the data necessary for the performance of activities and the timely provision of services, and to deal with peak orders, message or transaction volumes, as needed, including where new technology is introduced.	
	d) Use and maintain updated ICT systems, protocols and tools that are technologically resilient in order to adequately deal with additional information processing needs as required under stressed market conditions or other adverse situations.	

Articles For Pillar I: ICT Risk Management, cont'd		How Gigamon Helps
Identification **(Article 8)**	• **Security Policies:** Firms must implement comprehensive ICT security policies to protect their systems and data. • **Access Controls:** Firms need to establish strict access controls to ensure only authorised personnel can access critical systems. • **Data Protection:** Firms must protect sensitive data through encryption and other security measures. • **Incident Management:** Firms are required to have procedures for detecting, managing, and recovering from ICT security incidents. • **Continuous Monitoring:** Firms should continuously monitor their ICT systems for vulnerabilities and threats. • **Testing and Validation:** Regular testing and validation of security measures are necessary to ensure their effectiveness. • **Third-Party Management:** Firms must ensure that third-party service providers comply with similar ICT security standards to mitigate risks.	Gigamon provides a comprehensive suite of tools that can assist firms in meeting these requirements: **1. Security Policies** Gigamon strengthens security policies by delivering comprehensive insights into network traffic. Across physical, virtual, and cloud environments. This visibility allows organisations to enforce security policies effectively by identifying and understanding network behaviour, detecting anomalies, and ensuring that traffic adheres to predefined security rules. **2. Access Controls** The Gigamon Deep Observability Pipeline supports strict access control policies by monitoring all network traffic to ensure that only authorised users and devices are accessing critical systems. This can be achieved through integrations with network access control (NAC) solutions, identity and access management (IAM) tools, and by providing data for continuous monitoring of access patterns. **3. Data Protection** Gigamon helps in data protection by offering features like inline TLS/SSL Decryption, which allows security tools to inspect encrypted traffic for potential threats without compromising the data's confidentiality. By enabling real-time visibility into encrypted traffic, Gigamon ensures that sensitive data remains secure while allowing for effective threat detection and compliance with data protection regulations. **4. Incident Management** Gigamon enhances incident management tools and capabilities by providing detailed visibility into network traffic, which helps in the rapid detection of security incidents. It also aids in the analysis of incidents by capturing and storing traffic data, which can be used to investigate the cause, scope, and impact of security events. This accelerates response and recovery efforts. **5. Continuous Monitoring** Gigamon enables continuous monitoring of ICT systems by providing deep observability into network traffic across the entire infrastructure, be that public cloud, private cloud, virtual and/or on-prem. This includes network-derived intelligence for monitoring for vulnerabilities, threats, and anomalies, which helps organisations to detect potential security issues early and take proactive measures to mitigate risks.

Articles For Pillar I: ICT Risk Management, cont'd		How Gigamon Helps
Identification, cont'd **(Article 8)**	• **Security Policies:** Firms must implement comprehensive ICT security policies to protect their systems and data. • **Access Controls:** Firms need to establish strict access controls to ensure only authorised personnel can access critical systems. • **Data Protection:** Firms must protect sensitive data through encryption and other security measures. • **Incident Management:** Firms are required to have procedures for detecting, managing, and recovering from ICT security incidents. • **Continuous Monitoring:** Firms should continuously monitor their ICT systems for vulnerabilities and threats. • **Testing and Validation:** Regular testing and validation of security measures are necessary to ensure their effectiveness. • **Third-Party Management:** Firms must ensure that third-party service providers comply with similar ICT security standards to mitigate risks.	**6. Testing and Validation** Gigamon supports the regular testing and validation of security measures by allowing organisations to simulate attacks and monitor their defenses in a controlled environment. With traffic visibility and analysis, firms can validate the effectiveness of their security measures, identify weaknesses, and ensure that their systems are resilient against cyber threats. **7. Third-Party Management** Gigamon aids in third-party management by providing deep observability into the traffic between the firm's network and third-party service providers. This allows organisations to monitor the activities of third-party vendors, ensuring they comply with ICT security standards and do not introduce vulnerabilities into the firm's environment. Gigamon can also help in auditing and verifying third-party compliance with security requirements.

Articles For Pillar I: ICT Risk Management, cont'd		How Gigamon Helps
Protection and Prevention **(Article 9)** Detection, Response and recovery **(Article 10 & 11)**	Outline key requirements for firms to ensure their ICT systems are secure and resilient. **Article 8** mandates the implementation of comprehensive ICT security policies, including access controls, data protection, incident management, continuous monitoring, and third-party management. **Article 9** focuses on the reporting of significant ICT-related incidents, requiring firms to notify regulators promptly about any major disruptions or cyberattacks. **Article 10** emphasises the importance of regular digital operational resilience testing, such as vulnerability assessments and penetration tests, to ensure the effectiveness and security of ICT systems. These articles work together to strengthen firms' overall cybersecurity posture.	Gigamon enhances visibility, security, and monitoring capabilities specific to these articles: **Article 8 (ICT Security Policies):** Gigamon helps firms implement robust ICT security policies by providing deep observability into network traffic across physical, virtual, and cloud environments. This enables effective enforcement of access controls, real-time data protection through traffic inspection (including encrypted traffic), and comprehensive incident management by identifying and analysing threats quickly. Gigamon also supports continuous monitoring of vulnerabilities and threats, and facilitates oversight of third-party networks to ensure compliance with security standards. **Article 9 (Incident Reporting):** Gigamon enables rapid detection of significant ICT incidents by capturing and analysing network traffic in real-time. This visibility allows firms to quickly identify, classify, and respond to cyberattacks or disruptions, ensuring timely reporting to regulators as required under DORA. Gigamon also provides summarised and context-aware information for detailed forensics that can assist in incident investigations and regulatory reporting. **Article 10 (Resilience Testing):** Gigamon supports regular testing and validation of ICT systems by providing visibility into both encrypted and unencrypted traffic. This allows firms to assess the effectiveness of their security controls through vulnerability assessments, penetration testing, and simulations of potential threats. Gigamon offers traffic monitoring capabilities to ensure that security systems are working as intended and that any vulnerabilities are quickly identified and addressed, meeting DORA's resilience testing requirements.

Articles For Pillar I: ICT Risk Management, cont'd		How Gigamon Helps
Backup policies and recovery methods **(Article 12)**	Mandates that firms implement comprehensive backup policies and procedures to ensure the secure and timely restoration and recovery of critical data and systems following an ICT disruption or failure, minimising operational impact.	Gigamon helps with the backup, restoration, and recovery requirements of **Article 11** of DORA by providing deep observability into network traffic, which ensures that backup processes are functioning as expected and data integrity is maintained. In the event of an ICT disruption, real-time traffic monitoring and analytics from Gigamon enable rapid identification of affected systems, helping to streamline the recovery process and ensure secure, efficient data restoration. This visibility enhances the resilience and reliability of backup and recovery operations.
Learning and evolving **(Article 13)** Communication **(Article 14)**	Requires firms to continuously improve their ICT risk management by learning from past incidents, monitoring technological developments, and evolving their security measures to address emerging threats and vulnerabilities.	Gigamon helps with the backup, restoration, and recovery requirements of **Article 11** of DORA by providing deep observability into network traffic, which ensures that backup processes are functioning as expected and data integrity is maintained. In the event of an ICT disruption, real-time traffic monitoring and analytics from Gigamon enable rapid identification of affected systems, helping to streamline the recovery process and ensure secure, efficient data restoration. This visibility enhances the resilience and reliability of backup and recovery operations.
Harmonisation **(Article 15)**	Focuses on the further harmonisation of ICT risk management tools, methods, processes, and policies to enhance consistency and effectiveness in managing ICT risks across firms.	Gigamon provides standardised visibility and analytics solutions from on-prem to hybrid cloud that can be integrated across various ICT risk management tools and processes. This integration supports consistent monitoring, data collection, and threat analysis across different systems and environments, facilitating a unified approach to managing ICT risks and ensuring more effective and harmonised risk management practices.

Pillar II

INCIDENT MANAGEMENT

In compliance with DORA's second pillar on incident management, Gigamon enhances threat detection and response by providing comprehensive network visibility and real-time traffic analysis. The Gigamon Deep Observability Pipeline provides solutions that enable organisations to swiftly identify and analyse cybersecurity incidents, ensuring that they can respond effectively and meet DORA's requirements for timely and accurate incident reporting. By offering detailed insights into network activity, Gigamon supports rapid detection, efficient response, and thorough documentation of incidents, helping organisations adhere to regulatory mandates and strengthen their overall incident management processes.

Articles For Pillar II: ICT Related Incident Management		How Gigamon Helps
ICT-Related incident management process **(Article 17)**	Requires firms to establish and maintain a comprehensive ICT-related incident management process, including detection, response, and recovery procedures, to effectively handle and mitigate the impact of ICT incidents.	Gigamon aids in effective response by offering detailed insights into the nature and scope of incidents and facilitate recovery by supplying comprehensive data for forensic analysis and root cause identification. This comprehensive visibility helps firms manage and mitigate the impact of ICT incidents more effectively.
Classification of ICT incidents **(Article 18)** Reporting of ICT incidents **(Article 19)**	Requires firms to classify ICT-related incidents based on their severity and impact, mandating the prompt reporting of major ICT-related incidents to relevant authorities and stakeholders, including detailed information on the incident's nature and consequences.	Gigamon aids with classification of ICT incidents by providing detailed visibility into network traffic that helps firms accurately classify ICT-related incidents based on their severity and impact. Gigamon supports prompt and comprehensive reporting by delivering real-time analytics and detailed incident data, which helps firms quickly generate and share accurate reports with authorities and stakeholders, ensuring transparency and compliance.

Pillar III

DIGITAL OPERATIONAL RESILIENCE TESTING

The Gigamon Deep Observability Pipeline provides comprehensive network visibility and enables threat detection capabilities that are crucial for helping organisations meet the operational resilience requirements outlined in DORA's third pillar. By providing deep, real-time insights into network traffic and behaviour, Gigamon enables financial entities to continuously monitor their network environment, assess potential vulnerabilities, and detect threats. This ongoing visibility supports the adaptation and enhancement of cybersecurity measures, ensuring that organisations maintain compliance with DORA's standards for operational robustness and resilience. Gigamon can also facilitate proactive management of cybersecurity risks, helping firms stay aligned with regulatory requirements and bolster their overall operational resilience.

Articles For Pillar III: Digital Operational Resilience Testing		How Gigamon Helps
General Requirements **(Article 24)**	Perform digital operational resilience testing, ensuring that testing is comprehensive and effective. Including the Testing of ICT tools and systems to assess their resilience.	Gigamon provides visibility into network traffic consistently across private cloud, virtual, and on-prem environments including system interactions, which is essential for comprehensive and effective digital operational resilience testing. Gigamon solutions offer insights into how ICT tools and systems behave under various conditions, helping organisations evaluate their resilience and effectiveness during testing. This enhanced visibility ensures that testing processes are thorough and that any potential weaknesses are identified and addressed
Testing of ICT **(Article 25)**		

Pillar IV

THIRD-PARTY RISK

Gigamon supports financial organisations in this pillar by offering enhanced visibility into the activities of their third-party ICT providers. Gigamon offers network monitoring solutions that allow firms to gain detailed insights into the traffic and interactions involving these critical digital service contributors. This visibility enables organisations to effectively manage and secure their third-party relationships by identifying potential risks, monitoring compliance with security standards, and ensuring that these external providers do not introduce vulnerabilities into the firm's network. By providing comprehensive oversight, Gigamon helps financial entities maintain robust security and resilience in their third-party ICT arrangements.

Articles For Pillar IV: Managing of ICT Third-Party Risk		How Gigamon Helps
General Principles **(Article 28)**	Firms must ensure resilience and security across all ICT systems and processes. focusing on assessing ICT concentration risk and managing further sub-outsourcing arrangements to mitigate risks associated with over-reliance on specific ICT providers or third parties.	Gigamon helps ensure the resilience and security of all ICT systems and processes through detailed monitoring and threat detection. Gigamon assists in assessing ICT concentration risk by offering insights into traffic patterns and dependencies across different ICT providers and sub-outsourcing arrangements. This visibility helps identify and mitigate risks associated with over-reliance on specific providers, ensuring a more balanced and secure ICT ecosystem.
Assessment of ICT Concentration risk and further sub-outsourcing arrangements **(Article 29)**		
Key contractual provisions **(Article 30)**	Requires firms to include key contractual provisions in agreements with ICT third-party service providers to ensure compliance with security and resilience standards. Mandating the designation of critical ICT third-party service providers, identifying those whose failure or disruption could significantly impact the firm's operations and resilience.	Gigamon provides visibility into interactions with third-party service providers, helping firms ensure that their contractual provisions for security and resilience are being met. Gigamon helps identify critical ICT third-party service providers by monitoring and analysing traffic patterns, which assists in assessing the potential impact of their failure or disruption on the firm's operations and resilience. This visibility supports effective risk management and compliance with DORA requirements.
Designation of critical ICT third-party service providers **(Article 31)**		
Structure of the oversight framework **(Article 32)**	Outlines the requirements for structuring an oversight framework to manage and mitigate concentration risk by ensuring effective supervision and control over ICT third-party service providers and their impact on the firm's resilience.	By monitoring the network activities of ICT third-party service providers, Gigamon enables firms to maintain effective oversight and control, ensuring that potential risks, such as over-reliance on a single provider or vulnerabilities introduced by third parties, are identified and addressed. This visibility allows firms to assess the impact of third-party providers on their overall resilience and implement measures to mitigate any concentration risks, thus supporting the structuring of a robust oversight framework in compliance with regulatory requirements.

Pillar V

INFORMATION SHARING

The Gigamon Deep Observability Pipeline provides comprehensive network visibility and enables threat detection capabilities that are crucial for helping organisations meet the operational resilience requirements outlined in DORA's third pillar. By providing deep, real-time insights into network traffic and behaviour, Gigamon enables financial entities to continuously monitor their network environment, assess potential vulnerabilities, and detect threats. This ongoing visibility supports the adaptation and enhancement of cybersecurity measures, ensuring that organisations maintain compliance with DORA's standards for operational robustness and resilience. Gigamon can also facilitate proactive management of cybersecurity risks, helping firms stay aligned with regulatory requirements and bolster their overall operational resilience.

Articles For Pillar V: Information Sharing		How Gigamon Helps
Information sharing arrangements on cyber threat information and intelligence **(Article 45)**	Firms must establish processes for learning from both internal and external ICT-related incidents and engage in information and intelligence sharing with relevant stakeholders and industry bodies to enhance collective understanding and mitigation of ICT risks.	Gigamon helps firms establish processes for learning from ICT-related incidents and engage in information and intelligence sharing by providing comprehensive visibility and analytics into hybrid network traffic. This enables firms to capture detailed data on internal and external incidents, facilitating thorough analysis and understanding. Additionally, Gigamon solutions support effective information sharing by enabling the secure and efficient dissemination of threat intelligence to relevant stakeholders and industry bodies, enhancing collective risk mitigation and resilience.

Conclusion

In an increasingly complex and digitally-driven financial landscape, compliance with the Digital Operational Resilience Act (DORA) is critical for ensuring the stability, security, and resilience of financial institutions. This mapping guide has outlined how comprehensive network visibility and security solutions from Gigamon align with the key requirements of DORA, supporting firms in managing ICT risks, enhancing threat detection and response, and ensuring compliance with incident reporting and third-party risk management mandates.

By leveraging the Gigamon Deep Observability Pipeline, financial organisations can strengthen their digital operational resilience through continuous monitoring, advanced analytics, and secure data sharing. Gigamon plays a pivotal role in helping firms meet the regulatory requirements set forth by DORA while bolstering their ability to defend against evolving cyber threats and maintaining uninterrupted operations in a dynamic digital environment.

About Gigamon

Gigamon® offers a deep observability pipeline that efficiently delivers network-derived intelligence to cloud, security, and observability tools. This helps eliminate security blind spots and reduce tool costs, enabling you to better secure and manage your hybrid cloud infrastructure. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 8 of the 10 largest financial service organisations, and hundreds of governments and educational organisations.

To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

10.24_01