WHITE PAPER

Supporting DORA Objectives with Akamai

The concept of digital operational resilience has evolved significantly over the years, particularly within financial services. Initially, financial entities focused on disaster recovery and business continuity planning. These early efforts were primarily reactive, aiming to restore services after a disruption occurred. As cyberthreats became more prevalent and sophisticated, the focus shifted toward more proactive measures. Financial entities began implementing robust cybersecurity protocols, regular system updates, and employee training programs to prevent disruptions before they happen. The advent of advanced technologies such as large language models (LLMs), artificial intelligence (AI), and machine learning (ML) has revolutionized the approach to operational resilience. However, these same technologies have also revolutionized threat vectors, increasing the complexity and frequency of threats. As a result, operational resilience must continuously adapt to these evolving challenges.

These technologies enable predictive analytics, automated threat detection, and faster response times, significantly enhancing resilience capabilities. Increasing regulatory scrutiny has further driven the evolution of digital operational resilience. Regulations like the European Union (EU)'s General Data Protection Regulation (GDPR) have contributed to setting higher standards for data protection and operational continuity. However, the increasing complexity and frequency of cyberthreats are the primary drivers compelling financial entities to adopt more comprehensive resilience strategies. Modern approaches to digital operational resilience now encompass holistic risk management. This includes not only technical safeguards but also governance frameworks, third-party risk management, and continuous monitoring and improvement practices and information sharing.

Introduction to DORA

The Digital Operational Resilience Act (DORA) is an EU regulation aimed at enhancing the digital operational resilience of the financial services sector. It establishes a comprehensive framework for managing information and communications technology (ICT) risks and applies to a wide range of financial entities and ICT third-party service providers. Set to come into force on January 17, 2025, DORA mandates stringent requirements across five key pillars:

Risk Management

Incident Reporting

Digital Operational Resillience Testing

ICT Third-Party Risk Management

Information and Intelligence Sharing

DORA will bring increased regulatory requirements, requiring financial entities to meet stricter standards to ensure their operational resilience in the face of cyberattacks, system failures, and other digital risks. This will involve regular audits, compliance checks, and more rigorous reporting to regulatory bodies. Enhanced risk management will become a necessity as DORA mandates a comprehensive and integrated approach to identifying and assessing the risks associated with critical business services and digital systems. Financial entities will need to implement robust controls and continuously monitor and mitigate these risks. For many financial entities, complying with DORA will require greater investment in technology.

Financial entities will need to invest in advanced technologies, such as AI and ML, to improve and accelerate their operational resilience and response capabilities by providing better threat detection, automated responses, and predictive analytics. A focus on third-party risk management will also be crucial. Financial entities must ensure that their third-party service providers have robust operational resilience measures in place. This involves conducting thorough due diligence, performing regular assessments, and establishing clear contractual obligations to protect against digital risks. DORA also demands increased transparency. Financial entities will need to provide greater transparency around their operational resilience practices, demonstrating their ability to respond effectively to digital disruptions, maintaining comprehensive records, and communicating openly with regulators, stakeholders, and customers.

The importance of DORA for financial entities

DORA comes at a critical time for financial entities, addressing the increasing frequency and sophistication of cyberthreats. Over the past two decades, the financial services sector has been one of the most attractive targets for cybercriminals, according to the International Monetary Fund. The size of losses has more than quadrupled since 2017 to $2.5 billion, and indirect losses like reputational damage or security upgrades are substantially higher. Attacks have not only compromised sensitive financial information but have also posed significant risks to the overall stability and integrity of financial systems. As financial entities increasingly rely on digital infrastructure, the complexity and interconnectivity of their systems make them more vulnerable to cyberthreats. Attackers exploit these vulnerabilities, often using sophisticated techniques such as lateral movement within networks to gain access to valuable data or disrupt services. This method allows cybercriminals to traverse from one system to another, making it difficult to detect and prevent malicious activities, thereby increasing the potential for significant breaches or operational disruptions.

DORA's adoption is a proactive response to these evolving threats. By establishing a harmonized framework for digital resilience across EU member states, DORA aims to ensure a consistent level of security and operational resilience throughout the financial sector. This uniformity is crucial, as it enhances trust in the sector's digital infrastructure, ensuring that financial entities can withstand (and recover from) technological disruptions. The proactive nature of DORA reflects a strategic shift from merely reacting to incidents to anticipating and mitigating potential risks before they materialize. This approach is designed not only to protect individual entities but also to safeguard the broader financial ecosystem from systemic risks. The regulation's focus on enhancing incident response mechanisms and improving third-party risk management underscores the importance of a comprehensive and integrated approach to cybersecurity.

Transparency is another critical aspect of DORA. Financial entities must provide greater visibility into their operational resilience practices, demonstrating their ability to respond effectively to digital disruptions. This transparency is vital for maintaining the confidence of regulators, stakeholders, and customers, and it underscores the institution's commitment to protecting its digital infrastructure. The importance of DORA extends beyond regulatory compliance. It represents a fundamental shift in how financial entities approach cybersecurity and operational resilience. By aligning with DORA's requirements, financial entities not only protect themselves against current and future threats but also position themselves as trusted entities in an increasingly digital financial landscape.

How Akamai helps financial entities comply with DORA

Leveraging the scale of our global platform and its comprehensive threat intelligence, we help financial entities prevent, detect, and mitigate cyberthreats in both on-premises and cloud environments, enabling them to navigate the complexities of evolving regulatory compliance mandates. Our solutions help address each of DORA's key pillars — risk management, incident reporting, digital operational resilience testing, ICT third-party risk management, and information and intelligence sharing — ensuring comprehensive coverage and robust cybersecurity postures.

API Security

Akamai API Security offers comprehensive API discovery, posture management, and AI/ML–powered runtime protection, essential for detecting and blocking advanced API attacks in real time. Proactive security testing and real-time analytics enable financial entities to swiftly audit API behavior, respond to threats, and protect sensitive data, supporting compliance with DORA's ICT risk management and incident reporting requirements.

Mitigating risks associated with shadow APIs, vulnerable APIs, and API abuse is a significant challenge due to a lack of visibility and oversight. Effective API security provides comprehensive discovery and cataloging, real-time threat detection, and AI-driven protection mechanisms, ensuring continuous monitoring and mitigation of API-related threats and supporting compliance with DORA's regulatory standards.

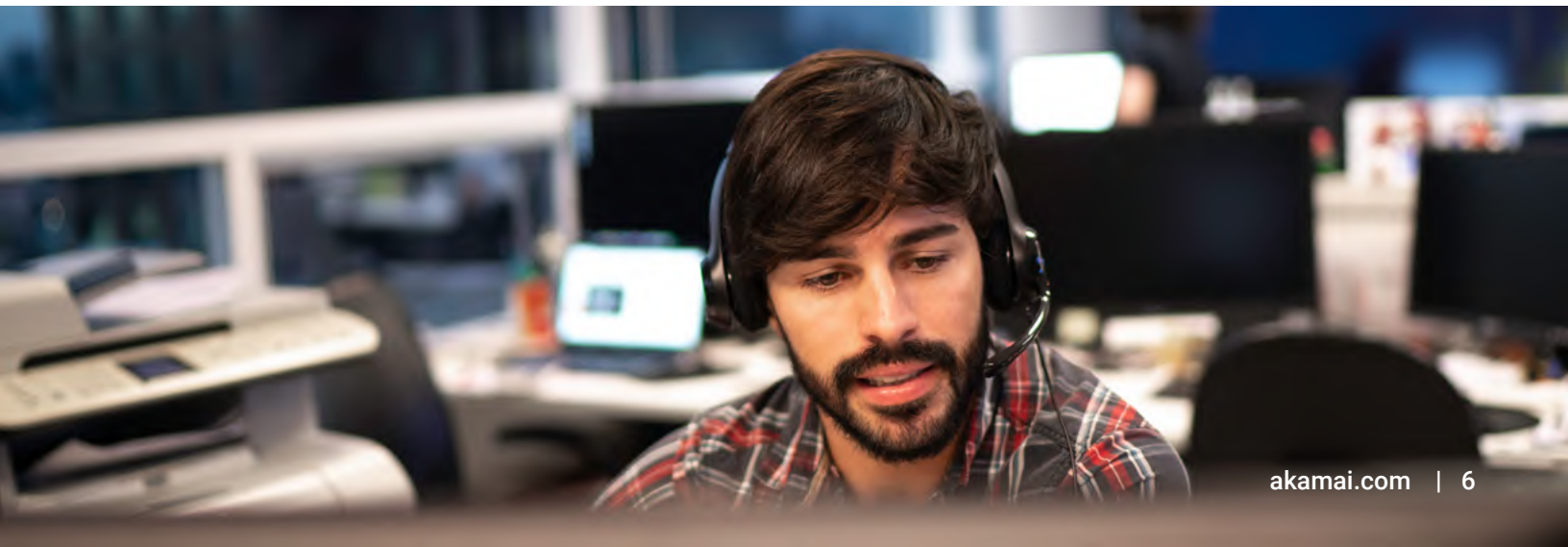
Akamai Guardicore Segmentation

Akamai Guardicore Segmentation allows financial entities to partition their networks into secure segments, significantly reducing the risk of lateral movement by cyberthreats. This technology aligns with DORA's objectives by enhancing ICT risk management and digital operational resilience testing. By isolating compromised assets and restricting adversaries' lateral movement, microsegmentation helps maintain a robust security posture and facilitates effective incident response.

Akamai Guardicore Segmentation offers deep visibility into application dependencies and precise policy enforcement, ensuring ongoing management of microsegmentation policies. The platform supports both agent-based and agentless deployment options, providing flexibility for various environments, including in-cloud PaaS, IoT, and OT environments. By leveraging AI-powered policy creation and intuitive workflows, Akamai Guardicore Segmentation simplifies the microsegmentation process, enabling financial entities to quickly implement and adapt security policies to changing network conditions. This comprehensive approach not only reduces the attack surface but also helps support compliance with regulatory requirements for digital operational resilience.

Edge DNS

Akamai Edge DNS ensures high availability and performance of DNS services, protecting on-premises, cloud, and hybrid DNS infrastructure. This solution is essential for maintaining service continuity and protecting against large-scale cyberthreats, addressing DORA's requirements for ICT risk management and incident reporting.



App & API Protector

Akamai App & API Protector combats Layer 7 attacks with comprehensive protections, including defense against distributed denial of service (DDoS), bots, and OWASP Top 10 exploits. This solution supports robust security for web applications and APIs, which is critical for complying with DORA's ICT risk management and incident reporting mandates.

Client-Side Protection & Compliance

Akamai assists with PCI compliance and protects websites against JavaScript attacks. This helps keep sensitive customer data safeguarded and helps financial entities meet stringent compliance requirements set forth by DORA and other regulations.

Prolexic

Akamai Prolexic protects infrastructure from DDoS attacks. It offers robust defense mechanisms to ensure uptime and reliability, even during large-scale attacks, thus supporting DORA's objectives of enhancing digital operational resilience and incident response capabilities.

Bot Manager

Akamai Bot Manager provides advanced bot management designed to detect and mitigate sophisticated bad bots while allowing good bots. This helps support legitimate traffic, maintaining a seamless user experience and helping companies adhere to DORA's ICT risk management requirements.

Account Protector

Akamai Account Protector detects and mitigates account takeover, account opening abuse, and credential stuffing. This capability is crucial for helping to protect customer accounts and maintaining trust, aligning with DORA's focus on robust ICT risk management and incident reporting.

Content Protector

Akamai Content Protector helps stop scrapers from stealing content and lowering conversion rates. This solution helps proprietary content remain secure, supporting DORA's objectives of safeguarding digital assets and enhancing operational resilience.

Detailed requirements and Akamai solutions

Governance and organization

Security governance: Akamai's Security Operations Command Center provides 24/7 monitoring and response services, helping to monitor security governance continuously.

Security information and event management (SIEM) integration: Akamai's SIEM integration solution provides a way to deliver SIEM events to analytic tools such as Splunk, QRadar, and ArcSight, allowing you to incorporate Akamai security events into your overall eventing and security infrastructure.

Governance, risk, and compliance (GRC): The Akamai Control Center provides a centralized interface for managing Akamai's products and services, offering businesses the access, insight, and control needed to help them meet risk, compliance, and regulatory requirements while delivering optimal online experiences.

ICT risk management framework

Risk management software: Akamai Secure Internet Access delivers advanced threat protection, including malware and phishing defenses.

Endpoint protection platforms: Akamai Bot Manager helps manage and mitigate malicious bot traffic.

Vulnerability management tools: Akamai's solutions provide continuous scanning and vulnerability assessment of ICT systems.

ICT-related incident management

Incident response platforms: Akamai's incident response services automate and orchestrate incident response processes.

Incident tracking systems: Akamai's solutions track and manage incident reports and resolutions.

Digital operational resilience testing

Penetration testing services: Akamai offers onboarded customer service pen testing and other security assessment services.

Red team/blue team exercises: Akamai conducts regular security exercises to assess and improve organizational response and achieve regulatory compliance.

Third-party risk management

Third-party risk management platforms: Akamai's security products, including web application firewall (WAF) and API Gateway, help manage and mitigate risks.

Contract management software: Akamai's solutions help manage contractual obligations and ensure compliance.

Threat intelligence platforms: Akamai's threat intelligence services provide up-to-date information on emerging threats using external and internal feeds.

Financial Services Information Sharing and Analysis Center (FS-ISAC): Akamai is the founding member of the FS-ISAC critical provider program. Internal collaboration and threat intelligence sharing continue to be key to successfully securing the infrastructure of the financial services industry through expeditious communication regarding vulnerabilities, outages, risks, or breaches. Our unique access to traffic and attack data enables us to partner on research and share best practices with members.

Oversight and enforcement

Audit and compliance tools: Akamai's compliance solutions help to audit and ensure adherence to regulatory requirements.

Monitoring and reporting solutions: The Control Center provides comprehensive monitoring and reporting capabilities.

Customer references demonstrating Akamai's effectiveness

To determine if Akamai is suitable for assisting with regulatory compliance, examining customer experiences can be insightful. Here are a few relevant cases:

Large insurance organization: This customer story highlights how this insurer leverages Akamai's solutions to enhance security and performance. Akamai's offerings help in mitigating DDoS attacks and securing APIs, which are crucial components for maintaining ICT risk management and incident response as required by DORA.

Cashflows: Cashflows uses Akamai's security solutions to protect its cloud-hosted payment platform. This case demonstrates how Akamai helps maintain compliance with security standards and protect against threats like DDoS attacks, ensuring continuous availability and security of payment services. This aligns with DORA's requirements for ICT risk management and digital operational resilience testing.

LANDBANK: As the largest government-owned bank in the Philippines, LANDBANK relies on Akamai to secure its online applications, protect against cyberthreats, and simplify its digital transformation. This story is particularly relevant for understanding how Akamai's solutions can help manage third-party risks and ensure robust incident management processes.

These examples illustrate how Akamai's comprehensive security solutions and proactive threat management capabilities can support financial entities in meeting DORA requirements, including ICT risk management, incident reporting, digital operational resilience testing, and third-party risk management.

Conclusion

DORA represents a significant shift in the regulatory landscape for financial entities, demanding comprehensive and proactive cybersecurity measures. Akamai's suite of solutions offers a robust framework for financial entities to help them (1) meet DORA's stringent requirements and (2) ensure enhanced digital operational resilience, robust ICT risk management, and effective incident response capabilities. By leveraging Akamai's advanced technologies, financial entities can confidently navigate the complexities of DORA compliance and safeguard their operations against the evolving threat landscape.

Learn more about our solutions for financial services

Akamai security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale and visibility of our global platform, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision.