AKAMAI SOLUTION BRIEF

Akamai for Financial Services — Your DORA Compliance Partner

The Digital Operational Resilience Act (DORA) is placing new requirements on how financial institutions manage ICT risks, cybersecurity, and operational resilience. Akamai offers a comprehensive suite of security solutions that can help financial institutions in their journey toward meeting DORA's requirements. This brief explains how Akamai's solutions help financial institutions meet regulatory demands, secure applications, and support long-term operational resilience and compliance.

How Akamai supports DORA compliance

Akamai offers a broad portfolio of security solutions that can help financial institutions address key aspects of DORA compliance while maintaining the performance and customer experience they expect. Our solutions provide robust protection for your applications and infrastructure, offering real-time threat intelligence and advanced security features that support continuous compliance efforts and operational resilience.

Here's how Akamai's solutions can help:

1. **Data protection and operational resilience:** Financial entities must secure sensitive data and ensure operational resilience. Akamai API Security helps achieve this by providing real-time visibility and monitoring, protecting APIs from misuse and breaches.
2. **ICT risk management:** DORA mandates effective management of ICT risks. Akamai Guardicore Segmentation isolates key applications, preventing lateral attack movement and improving infrastructure resilience.
3. **Resilience of DNS infrastructure:** The security and availability of DNS services are vital for operational continuity. Akamai Edge DNS secures cloud-based and hybrid DNS infrastructure.
4. **Application and API security:** Applications and APIs must be protected from cyberthreats. Akamai App & API Protector shields apps and APIs from DDoS, bot attacks, and vulnerabilities for secure, uninterrupted performance.
5. **Client-side data security:** Financial entities must secure client-side data and ensure compliance with standards like PCI DSS. Akamai Client-Side Protection & Compliance safeguards websites from JavaScript attacks, helping to keep customer data secure.
6. **Incident management and testing:** DORA requires resilience testing and incident response capabilities. Akamai Prolexic defends against DDoS attacks to protect uptime.

Key steps to consider

1. Conduct initial review of DORA.
2. Establish DORA project team.
3. Conduct detailed review of DORA and its standards.
4. Map current state against DORA.
5. Conduct options analysis.
6. Create project plan.
7. Implement plan and complete DORA project.

7. **Customer protection:** Protecting customers from account takeover and ensuring seamless experiences are crucial. Akamai Bot Manager and Akamai Account Protector safeguard accounts by detecting fraudulent activity and mitigating bad bots.
8. **Protection of digital assets:** Financial entities must secure their digital assets and proprietary information. Akamai Content Protector prevents content scraping.

Key benefits of Akamai for supporting DORA compliance

Akamai solutions help financial institutions address key aspects of DORA requirements while securing applications and infrastructure across key areas:

Regulatory alignment: Akamai's tools can support real-time risk management, incident response automation, and third-party risk visibility, helping financial institutions align with DORA's core objectives.

Threat intelligence sharing: As a founding member of the FS-ISAC Critical Providers Program, Akamai collaborates with financial institutions to provide real-time insights into emerging threats, contributing to industry resilience.

Protecting applications everywhere: Akamai helps secure application workloads and infrastructure from abuse and cyberthreats, supporting seamless protection and DORA compliance without compromising performance.

ROI and cost-benefit analysis

Reduce regulatory risk: Help reduce the risk of regulatory penalties by using Akamai's solutions to support your DORA compliance efforts.

Minimize downtime: Strengthen protection against cyberthreats to help keep your business operational and protect revenue.

Lower security costs: Consolidate security needs with Akamai to reduce the complexity and expense of managing multiple vendors.

Adapt to evolving regulations: Akamai's scalable platform helps financial institutions adapt to changing regulatory requirements, potentially reducing the need for significant reinvestments.

Why choose Akamai?

1. **Industry-leading security platform**
   Akamai's global platform offers unparalleled visibility and protection across on-premises, cloud, and hybrid environments. Leveraging advanced machine learning technologies, our solutions detect and mitigate threats in real time, ensuring your institution remains secure from the most advanced cyberthreats.
2. **Proven track record in financial services**
   Akamai is trusted by 9 of the top 10 global banks and leading financial institutions worldwide.

DORA introduces new requirements, such as those for critical third-party providers (CTPPs), and is more detailed and specific than many other regulations that are often more principle based.

The five pillars of DORA

1. Risk management
2. Incident reporting
3. Digital operational resilience testing
4. ICT third-party risk
5. Information and intelligence sharing

3. **FS-ISAC Critical Providers Program**
   As a founding member of the FS-ISAC Critical Providers Program, Akamai plays a pivotal role in strengthening the financial services sector's cybersecurity. The program fosters continuous collaboration between FS-ISAC member firms and financial institutions, helping to secure network infrastructure and protect against emerging threats. Our commitment to the global sharing of threat intelligence ensures that financial institutions are well equipped to face the constantly evolving cyberthreat landscape.

4. **Comprehensive support and expertise**
   Akamai provides 24/7/365 expert support to protect your institution around the clock. Our team of cybersecurity professionals offers personalized assistance at every step of your journey.

   Exceptional support
   Guaranteed uptime and performance: Akamai's SLAs guarantee uptime and performance, even during large-scale attacks, ensuring smooth operations.

   Advanced threat intelligence
   Akamai's global platform provides real-time updates on emerging threats, keeping your institution ahead of cybercriminals with proactive defense.

   Dedicated account management
   Akamai offers dedicated account managers and support teams to assist with compliance efforts, security audits, and technical challenges, delivering personalized support tailored to your needs.

Akamai's security solutions support financial institutions by enhancing security, operational resilience, and cost efficiency. With advanced security capabilities like API protection, DDoS defense, and microsegmentation, your institution is better equipped to meet DORA's regulatory requirements while safeguarding the applications and infrastructure that power your business. Additionally, as a member of the FS-ISAC Critical Providers Program, Akamai is uniquely positioned to offer real-time threat intelligence sharing, helping your institution stay ahead of emerging risks.

To learn more, visit akamai.com or contact your Akamai sales team.

| Published 12/24