AKAMAI BRIEF

Digital Operational Resilience Act

Preparing financial entities for DORA compliance with Akamai

The Digital Operational Resilience Act (DORA) is a new major piece of European legislation that sets a stronger regulatory rulebook for regulated financial entities by requiring an enhanced digital operational resilience framework covering not only financial entities but also their Information and Communication Technology (ICT) third-party providers. DORA will come into force on 17 January, 2025.

DORA scope

DORA applies to financial entities globally that operate in EU markets. The scope includes traditional entities like banks, investment firms, and credit institutions, as well as nontraditional ones such as crypto-asset service providers and crowdfunding platforms.

Moreover, DORA provides certain obligations on entities that are not financial entities and generally exempt from financial regulations. For instance, third-party service providers supplying financial firms with ICT systems and services — such as cloud service providers and data centers — must comply with certain DORA requirements. Additionally, DORA encompasses firms providing critical third-party information services, like credit rating services and data analytics providers. ICT third-party providers that are designated as critical by the European Supervisory Authorities (ESAs) will be under assessment by a lead overseer appointed by the ESAs.

Akamai will support financial authorities' objectives and provide assistance both as a critical third party and as a vendor, assisting in meeting expected framework regimes by our customers. We will cooperate in providing assistance with inquiries and help understand means by which we provide operational resilience.

DORA's 5 pillars

DORA's comprehensive approach is built upon five pivotal pillars, each tailored to address distinct facets of digital operational resilience.

Risk Management | Incident Reporting | Digital Operation Resiliency Testing | ICT Third-Party Risk | Information and Intelligence Sharing

Risk Management

- Complete visibility into service performance using Akamai Control Center (ACC) and its embedded security analytics dashboards, SLA monitoring, and insight into documentation, including policies and reports.
- Contractual-based third-party risk management assessments conducted annually on Akamai allow insight into company security and assess risks associated with service.
- Akamai Zero Trust and segmentation products help customers minimize and alleviate their risks related to ransomware and internal access elevation threats.
- Continuous auditing of Akamai security using industry and regional security frameworks such as SOC 2, ISO 27001, or German BSI allow better assessment of company risk status.

Incident Reporting

- 24/7 coverage with notification system for all customer-impacting incidents within expected timelines.
- Global coverage, with customer service and security specialists on standby in multiple operation centers in all major geographies.
- Provision of incident information via akamaistatus.com, community service, and ACC.

Akamai

Digital Operational Resiliency Testing

- State-of-the-art resiliency model tested in resisting the biggest DDoS attacks that the ICT industry has seen.
- Organized quarterly testing of infrastructure and semiannual testing of personnel readiness for recovery in case of disasters.
- Ongoing lessons learned and improvements implemented year after year to ensure Continuous internal and compliance-based penetration testing regime aligned with TIBER-EU third-party threat-led penetration tests assessing existing resiliency model.

ICT Third-Party Risk

- Akamai is assessing all its vendors and third parties before onboarding them and using their services and platforms. Every vendor and product undergoes specific checks related to its service security, the way it processes information, compliance with privacy law, and whether financial status of the company poses any risks for Akamai.
- Dedicated third-party risk management (TPRM) team ensures that vendors contractually comply with Akamai's vendor rules of engagement. Each critical vendor is subject to annual monitoring of compliance with contractual obligations, and exit plans are set in place in case of noncompliance.

Information and Intelligence Sharing

- Akamai Security Intelligence Group conducts continuous research on emerging threats aimed at ICT providers and Akamai customers. A sophisticated network of honeypots and intelligence gathered outside of Akamai's globally distributed edge is used to identify indicators of compromise (IOCs), which are later shared over different communication channels.
- Akamai is participating in the intelligence sharing community of FS-ISAC, contributing TLP Green and Amber intelligence samples and case studies.

"Financial entities shall have a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience." (Article 6)

The operational resilience framework necessitates ongoing attention to safeguard the organization's ICT and information assets. This includes continual protection of software, physical equipment, and data. The framework requires regular updates, at least annually, triggered by major ICT incidents, supervisory directives, or insights from testing or audit processes.

How Akamai helps

Akamai aligns with the authorities' objectives for a robust European financial system and values ongoing dialogue. We diligently comply with regulations and will assist customers in understanding our critical third-party approach while enhancing their operational resilience.

With Akamai, financial institutions can effectively manage compliance challenges, including regulatory ambiguity and uncertainty — whether DORA or future mandates — through comprehensive security measures spanning application workloads and APIs to app infrastructure. Security then becomes a vital component of the regulatory toolkit, facilitating sustainable, effective change, and, most importantly, fostering customer trust in financial institutions and the broader financial market.

Learn more about DORA.

 | Support | | Published 06/24