Hitachi Vantara

eBook

Simplify DORA Compliance with Hitachi Vantara

Deploy a defense-in-depth operational resilience solution, proven to accelerate DORA compliance for banking and financial services firms — reducing risk faster and at lower cost than multi-vendor alternatives

The Digital Operational Resilience Act (DORA) establishes strict Information Communication Technologies (ICT) resilience standards for financial institutions and their third-party ICT providers operating or transacting in the EU, effective January 2025. Aimed at protecting Europe's financial stability, DORA ensures firms can withstand and recover from ICT disruptions. This eBook outlines DORA's requirements, compliance benefits, and risks of non-compliance, including fines and client loss. It also provides a global regulatory context, with standards like DORA emerging in New York, Japan, Canada, the UK, and Australia—highlighting the need for global financial firms to adopt resilient operational practices for future-proof compliance.

Discover how Hitachi Vantara simplifies DORA compliance with a defense-in-depth approach, offering tailored assessments, remediation, and end-to-end solutions aligned with DORA's requirements—all from one trusted partner. With over 15 years in the financial sector, Hitachi delivers unbreakable operational resilience that reduces risk and achieves compliance faster and at less cost than multi-party solutions.

Table of Contents

What is DORA?

DORA is an EU regulation, effective January 2025, designed to reduce ICT-related risks in financial institutions that threaten Europe's financial system stability. DORA mandates rigorous standards for EU and non-EU banks, insurers, investment firms, and third-party ICT providers operating or transacting within the EU to withstand and recover from ICT disruptions, enhancing sector-wide resilience. Implementing DORA is not just about compliance; it's about transforming your operational resilience strategy to effectively protect against future threats – and recover from them.

Who must comply with DORA?

Financial Services Industry

- Payment institutions
- Investment firms
- Insurance companies
- Credit rating agencies
- Crypto-asset service providers
- Crowdfunding service providers
- Data analytics and audit services
- Fintech
- Trading venues
- Financial system providers
- Credit institutions

Third-Party ICT Service Providers

- Cloud service providers
- Data analytics providers
- Data centers
- Digital technology system providers
- Data service system providers

Why should you act?

78% *of EU financial institutions covered by DORA experienced a third-party data breach in the past year*

Source: SecurityScorecard

DORA compliance is essential for financial firms to strengthen cybersecurity and operational resilience, especially as 78% of EU financial institutions covered by DORA experienced third-party breaches in the last year, highlighting the need for improved security posture.

Non-compliance risks fines up to 1% of average daily worldwide turnover, reputational damage, and client loss. For ICT third-party providers, compliance is crucial to retain customers. Failing to support customers' compliance efforts can lead to lost revenue as they turn to compliant providers. Financial institutions and their third-party providers must act fast to achieve compliance by January 2025 and provide compliance testing attestation every three years thereafter.

DORA is shaping global operational resilience standards. With the 2023 implementation of 23 NYCRR Part 500 for all financials firms registered in New York State, Japan's Economic Security Promotion Act for essential infrastructure providers in the financial sector, and forthcoming regulations in Canada, the UK, and Australia, compliance is becoming essential for Fortune 1000 financial firms and their third parties. Aligning with DORA helps organizations meet current regulations and future-proof their infrastructure, preparing for global standards while enhancing long-term resilience, credibility, and competitiveness in a dynamic digital landscape.

How Hitachi Can Help: DORA Compliance Journey

One Partner. Assessment to Implementation.

For over 15 years, Hitachi has helped leading banks and financial firms manage emerging threats, complex regulations, and eDiscovery challenges to reduce operational and compliance risk. Our defense-in-depth solution accelerates your DORA compliance journey at a lower cost than engaging multiple consultants and technology providers. As a DORA-compliant third-party, we support governance, operational resilience evidence, and testing, reducing your compliance burden.

The result?

Faster, more affordable DORA compliance without the complexity of multi-party solutions.

Our Process

Gap Assessment

Collaborate with our cyber resilience, GRC, and financial services experts to assess your organization's security and DORA compliance risks through a proprietary gap and business impact assessment based on ISO 27001 and NIST 2.0.

Recommendation

Receive a no-obligation, actionable risk profile and a prioritized remediation roadmap covering policies, procedures, and technology and monitoring investments.

Remediation

Align your organization around a unified remediation plan with a Hitachi-led workshop. Hitachi deploys a tailored defense-in-depth solution—including hardware, software, and services—supported by our extensive ISV ecosystem.

How Hitachi Can Help: DORA Chapter II

ICT Risk Management & Governance

DORA mandates financial entities implement a resilient ICT risk management framework with continuous threat detection, response, and 2-hour recovery across their organization and supply chain. Management must oversee documented strategies to protect assets, control risks, and ensure business continuity.

Hitachi provides threat:

Governance

Augment your team with trusted GRC and CISO-as-a-Service solutions, providing expert guidance and education for C-level leaders to protect digital assets and ensure continuity, from tailored strategy development to execution.

Identification

Deploy proactive cyber threat mitigation with comprehensive vulnerability assessments and testing performed during off-peak times, within SDLC, or Thin Digital Twin environments, safeguarding your business and production environment from risk.

Protection

Protect your data across edge-core-cloud with data at rest and in motion encryption, key management, and access controls. Our FIPS 140-2 and 140-3 certified infrastructure employs immutable snapshots to prevent data loss, safeguarding against unauthorized changes, damage, and deletion.

Detection

Identify environment intrusions with AI-driven anomaly, malware, and ransomware detection, backed by 24/7 MDR from global SOCs. Gain peace of mind with industry-leading ransomware accuracy and protection through our Cyber Resilience Guarantee.

Response & Recovery

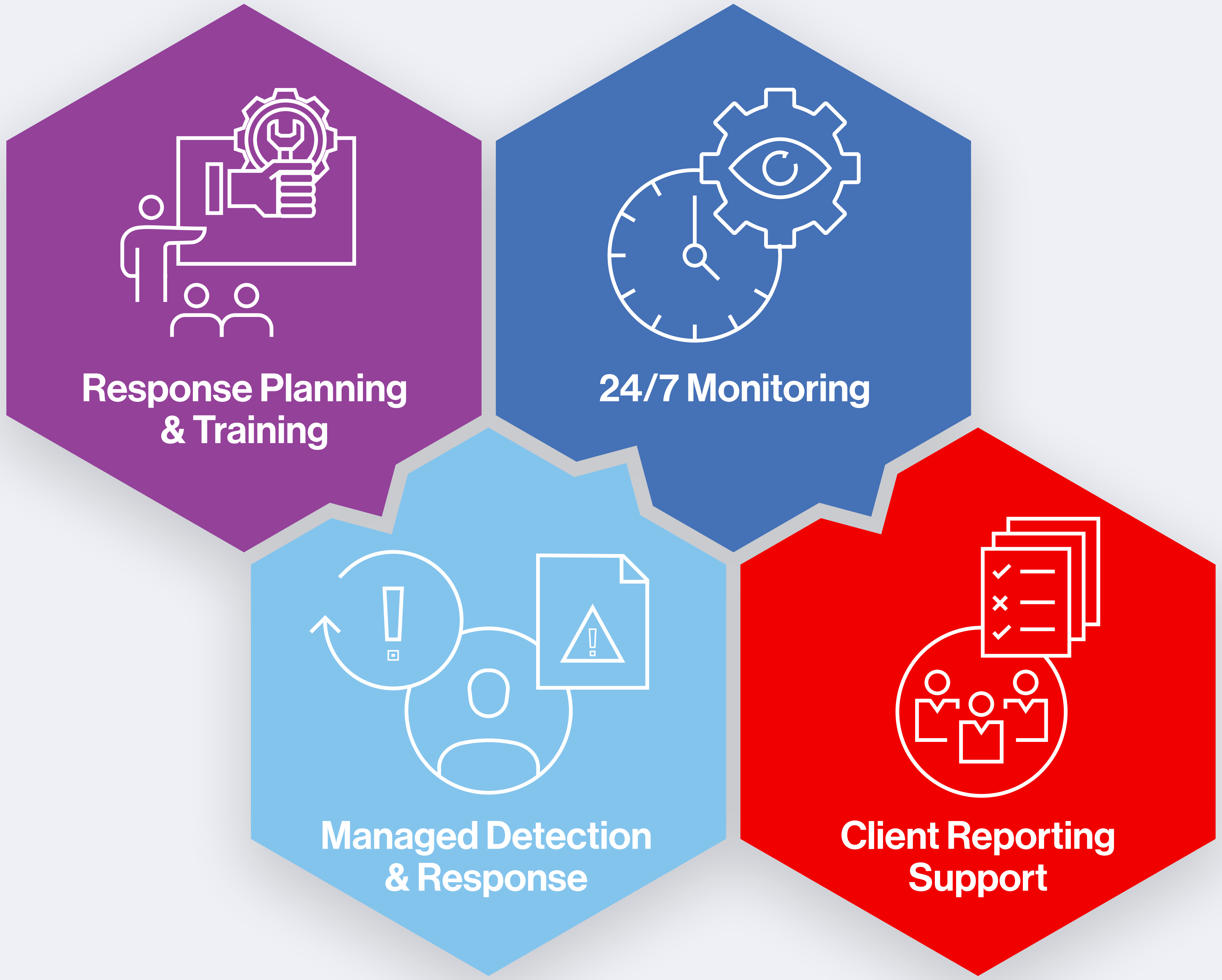
Ensure business continuity with scalable storage offering 100% data availability, the fastest ransomware recovery, and near-zero RTO/RPO. Protect data integrity with immutability, replication, and automated recovery, cutting disaster recovery time by up to 95%.

How Hitachi Can Help: DORA Chapter III

Incident Management & Reporting

Under DORA, financial firms must establish an ICT incident management framework, including prompt incident reporting to regulators, classification thresholds, and client notifications.

Hitachi supports DORA compliance with comprehensive incident management, including tailored response planning, training, 24/7 monitoring, and managed EDR and NDR services for real-time threat detection across endpoints, cloud, and enterprise infrastructure. Our solutions minimize disruption, ensure swift recovery, and, with CISO-as-a-Service, provide strategic client reporting to keep your business resilient and compliant.



How Hitachi Can Help: DORA Chapter IV

Digital Operational Resilience Testing

DORA mandates regular ICT disruption resilience testing. Firms must establish a structured testing program, including certified Threat-Led Penetration Testing (TLPT) every three years, to address identified vulnerabilities.

Hitachi designs tailored testing programs for critical, production, and third-party systems, aligned to your firm's size and risk profile. Using AI-driven and human Cyber Threat Intelligence with expert-led simulations, including red and white-teaming TLPT based on the TIBER-EU framework, we deliver in-depth risk mitigation. Strengthen defenses, protect your brand, and ensure resilience with Hitachi's comprehensive testing solutions.

How Hitachi Can Help: DORA Chapter V

Third-Party Risk Management

DORA mandates financial firms rigorously manage ICT third-party risks through thorough threat analysis, standardized contracts, due diligence, and regular reporting to regulators, ensuring robust oversight and alignment with regulatory requirements.

Hitachi supports DORA's third-party risk management with CISO-as-a-Service, helping to map and classify ICT providers, define oversight strategies, and streamline partner processes. We assess risk profiles, create remediation roadmaps, and manage vulnerabilities within your supply chain to reduce risk to your business and clients.

How Hitachi Can Help: DORA Chapter VI

Information Sharing

DORA encourages secure information-sharing among financial entities to strengthen cyber resilience, prevent ICT incidents, and enable faster recovery, fostering a collective defense against cyber threats across trusted industry networks monitored by regulators.

Hitachi supports DORA compliance by promoting secure intelligence sharing with peers and third-party providers. Our AI-driven Cyber Threat Intelligence, training and awareness programs, and secure data-sharing protocols enable proactive threat mitigation and help maintain trust with regulators and customers.

Why partner with Hitachi?

Achieve Compliance Risk Reduction

European public financial entity achieved DORA critical requirement compliance

Read the customer story →

Multinational financial services firm achieves regulatory reporting requirements, saves $3M annually

Read the customer story →

Why partner with Hitachi?

Achieve Unbreakable Operational Resilience

Ready to get started?
Contact a Hitachi cybersecurity expert.

Connect now →

DORA mandates operational resilience best practices for financial services firms transacting in the EU to ensure ICT disruption resilience. Non-compliance risks fines and client loss, underscoring the need for robust protections amid financial firm third-party breaches. DORA sets a standard for proliferating global regulation requirements.

Simplify DORA compliance with a comprehensive, single-vendor solution:

- **Reduce compliance complexity** while reducing storage TCO 20% or more with a defense-in-depth solution spanning hardware, software, and services.
- **Accelerate compliance risk reduction** with one partner for fast-to-market DORA gap assessment, remediation roadmap, and solution implementation.
- **Future-proof your investment** with a third-party validated solution for financial services data security and data privacy compliance standards.
- **Get peace of mind.** Deploy a solution trusted by 9 of the top 10 global banks and 10 of the top 10 insurers for unbreakable operational resilience and the industry's only 100% Data Availability Guarantee.
- **Keep your business running round-the-clock.** Cut downtime by up to 95%, to minutes with business continuity and the market's fastest ransomware recovery solutions backed by a Cyber Resilience Guarantee.

Hitachi Vantara

About Hitachi Vantara

Hitachi Vantara is transforming the way data fuels innovation. A wholly owned subsidiary of Hitachi Ltd., we're the data foundation the world's leading innovators rely on. Through data storage, infrastructure systems, cloud management and digital expertise, we build the foundation for sustainable business growth.

Corporate Headquarters
2535 Augustine Drive
Santa Clara, CA 95054 USA
hitachivantara.com | community.hitachivantara.com

Contact Information
USA: 1-800-446-0744
Global: 1-858-547-4526
hitachivantara.com/contact

PREVIOUS HOME