Hitachi Digital Services

Accelerating **DORA** compliance

The Digital Operational Resilience Act

What is the Digital Operational Resilience Act?

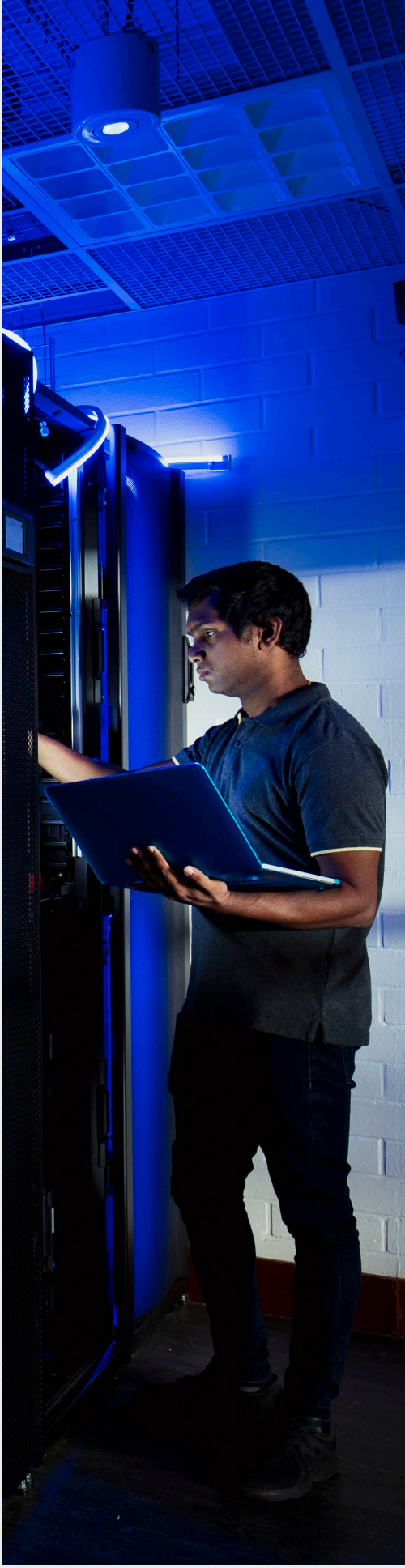
The financial sector's growing reliance on technology and tech companies makes financial entities increasingly vulnerable to cyberattacks. The risk is significant - if not well managed, the impacts of cyberthreat incidents can reach across borders, disrupting economies. The Digital Operational Resilience Act (DORA) was introduced in 2023 by the European Union (EU) to strengthen digital operational resilience in the EU financial sector. It defines an information and communications technology (ICT) risk management framework that financial entities and their technology partners must implement by January 17, 2025.

DORA presents robust processes for tackling cyber security and digital risk. Its goal is to equip EU Financial Services to better withstand, respond to and recover from ICT-related disruptions and threats.

Who does DORA apply to?

- Credit Institutions
- Payment Institutions
- Audit Firms
- Brokers Agencies
- Pension Institutions
- Crypto-asset Providers
- Investment Firms
- Crowdfund Services
- Credit Agencies
- Insurance Firms
- Service Integrator Partners
- Software Providers
- Cloud Service Vendors
- Data and Analytics Providers
- Service Providers

Key: Financial ICT



How does this impact you?

The DORA regulations set the bar for risk and resilience management. To implement them, you will need to focus on all five pillars of DORA.

Risk Management (ICT)

This pillar focuses on the adoption of ICT governance and control frameworks to reduce the probability of cyberattacks and improve recovery. It requires a clear view of critical functions and an understanding of risk exposure and impact tolerance. It extends ownership of risk management to both operational and security teams.

What you can do now:

1. Refine your risk management framework (identify, classify)
2. Build your risk procedure and recovery plan (manage)
3. Prepare your people to manage and react to an incident

Incident Reporting

Detailed reporting of ICT incidents will be required going forward. This will include impacts on users and data, notifications to relevant authorities, and identification of root causes. With robust knowledge around incidents and continuous improvements to prevent and recover from them, repeat incidents can be minimized.

What you can do now:

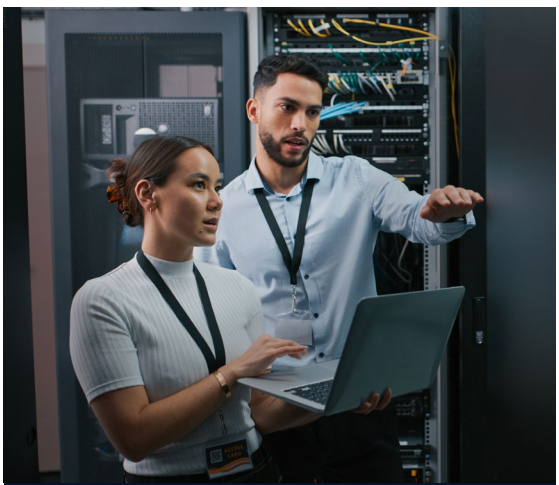
1. Review your incident reporting standards
2. Build robust incident management process ownership
3. Clearly communicate incident management strategies for both internal and external channels

Digital Operations Resilience Testing

This encompasses threat-based penetration testing, planning and execution by third-party providers. The frequency of operational resilience tests and advanced threat-led penetration tests should be appropriate to the risk profile of assets. Evaluations should always be carried out by an independent body.

What you can do now:

1. Create your threat-led penetration test strategy
2. Consider adopting and certifying an existing framework such as TIBER-EU
3. Scope requirements and draft a plan of engagement with vendors



DORA provides a harmonised set of regulations, ensuring **operational resilience**

Third-party Risk

Active management of third-party risk and appropriate contract design will support identification and adoption of the right level of risk management. To achieve this, clearly define your third-party landscape and build a robust audit process with an up-to-date third-party information register.

What you can do now:

1. Define your partner strategy and policy
2. Create a third-party register and landscape overview
3. Start audit cycles / information assessments

Information Sharing and Reporting

Financial entities will be required to report their adherence to DORA regulations to authorities and share intelligence between themselves. This will increase threat knowledge and defense capabilities. Guidelines to support stable communications have been shared.

What you can do now:

1. Participate in appropriate forums
2. Develop solutions on information sharing
3. Define your approach on consuming information

Hitachi DORA Compliance Framework

Hitachi's "DORA Compliance Framework" enables customers to accelerate their compliance program. Our "Compliance Advisory, Compliance Build Platform and Continuous Compliance Management" services helps customers meet where they are in their DORA compliance journey.

ICT Risk Management Framework

- Establish a strong governance model to oversee the program.
- Formulate and implement an ICT risk management framework
- Perform security maturity assessment aligning to DORA standards.
- Design and Build a resilient platform using 5C model and Zero-Trust Principles.
- Enforce Data-centric security approach

ICT-related incidents

- Provide Continuous Compliance Management through ongoing assessment and continuous monitoring.
- Develop, implement and maintain a robust IT security plan.
- Establish an engineering-led operations approach
- Provide a modern SOC service using threat-led intelligence and automated response.

Digital Operational Resiliency Testing

- Establish an end-to-end testing strategy that validates the operational resiliency and security effectiveness
- Resilience tests designed through a structured FMEA analysis process.
- Implement security chaos engineering principles to inject fault and test resiliency.
- Measure strength of observability controls, isolation controls, recovery controls and SLO compliances

ICT Third-party risk

- Perform assessment and analysis of service providers based on services rendered and concentration risk.
- Evaluate if third-party providers comply with high compliance standards and industry security best practices.
- Develop mitigation strategies for high-risk vendors through additional monitoring and controls.
- Review contracts, termination and exit plans

Information & Intelligence sharing

- Establish process to raise awareness and minimize spread of ICT risks.
- Create communication channels to notify competent authorities
- Exchange of Cyber threat intelligence including IOCs, tactics, techniques and security alerts.

How can Hitachi Digital Services help?

Hitachi Digital Services can support your entire journey to DORA compliance - from assessment to implementation of appropriate data storage and digital solutions to ensure you meet the requirements. If you have already started your Operational Resilience Program, we can help you leverage the processes and technologies introduced by DORA.

The new requirements introduced by DORA will demand substantial investment in the governance, risk and compliance frameworks around ICT, cyber and third-party risk management functions. Follow-on work will be necessary to address any operational vulnerabilities that are identified.

Review your status in terms of compliance of your

- Operational model
- Testing proficiency
- Incident management
- Third-party landscape
- Cloud strategy

Define a roadmap to reach your desired state of compliance

- Quick operational wins
- Training needs
- Infrastructure planning
- Software transition plan
- Reporting

Support your implementation

- Standardise operations
- User training
- Hardware support
- Software development
- Playbooks

References

1. EU - Regulation - 2022/2554 - EN - DORA - EUR-Lex
2. RTS - ICT Risk Management Framework
3. RTS - ICT services supporting critical or important functions
4. RTS - Classification of major incidents and significant cyber threats
5. RTS - Register of Information

About Hitachi Digital Services

Hitachi Digital Services, a wholly owned subsidiary of Hitachi Ltd., is an edge-to-core digital consultancy and technology services provider helping organizations realize the full potential of AI-driven digital transformation. Through a technology-unified operating model for cloud, data, and IoT, Hitachi Digital Services' end-to-end value creation for clients is established through innovation in digital engineering, implementation services, products, and solutions. Built on Hitachi Group's more than 110 years of innovation across industries, Hitachi Digital Services helps to improve people's lives today and build a sustainable world tomorrow. To learn more, visit hitachids.com

HDS-KIN-SP-Accelerating DORA compliance-20Feb24-B

European Headquarters: 14th floor, Broadgate Tower, 20 Primrose Street, London, EC2A 2EW

Hitachi Digital Services