



FOUR ACTIONS TO BECOME DORA COMPLIANT

A guide for financial services firms to achieve
digital operational resilience before 2025



INTRODUCTION

The Digital Operational Resilience Act (DORA) is a major piece of European Union legislation on cybersecurity for financial entities. It has been created to enhance the digital operational resilience of the EU financial services sector by strengthening financial entities' Information and Communication (ICT) and third-party risk management and reporting framework.

The regulation came into force on 16 January 2023, with a compliance deadline set for 17 January 2025. This leaves financial firms with little under a year to align themselves with the requirements of DORA and, critically, keep their organization one step ahead of constantly evolving threats.

However, becoming compliant doesn't have to be overwhelming. With this straightforward action plan and ECI's comprehensive Governance, Risk & Compliance (GRC) services, we can be the tried and trusted MSSP to increase your firm's digital operational resilience and turn compliance into business advantage.

WHAT DOES 'DIGITAL OPERATIONAL RESILIENCE' MEAN?

According to calculations from insurers Lloyd's, if a cyberattack on a major financial services payment system were to occur, the global loss could reach \$3.5 trillion (EUR €3.2 trillion) over a five-year period.¹ This reinforces how important it is for financial firms to ensure that the services they provide are not disrupted by cyberattacks, outages, or other risks that can compromise their integrity or continuity.

To quote the DORA text (3.1), digital operational resilience is "the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions".²

This means establishing an approach that matures beyond cyber defense to the ability to resist disruptions, incidents, and attacks.

¹Lloyds.com, ²DORA.com

DOES EVERY FINANCIAL FIRM NEED TO ADHERE TO DORA?

Firms that employ more than 10 persons and have a turnover and/or annual balance sheet total that exceeds EUR €2 million are required to be DORA compliant.

How does DORA define a major incident or significant threat?

Within the DORA framework, several sections refer to “major ICT incidents” and “significant cyber threats.” It is important to establish how the regulations classify these:

A major ICT incident is defined (3.10) as:

“one that significantly impacts the network and information systems supporting critical or important functions of a financial entity.” This generally means those which can impact your clients’ financial interests.

These incidents must be classified according to:

- The number and/or relevance of clients or financial counterparts affected.
- The duration of the incident.
- The geographical spread.
- The data losses entailed.
- The criticality of the services affected.
- The economic impact.

A significant cyber threat is defined (3.13) as

one that: “indicates potential to result in a major ICT-related incident or significant operational or security payment-related incident.”

What are the consequences of non-compliance?

DORA allows member states to determine appropriate sanctions for non-compliance, such as financial penalties.

These can include:



Firms found in violation of the Act may face fines of **up to 2% of their total annual worldwide turnover.**



In the case of an individual, **a maximum fine of EUR €1,000,000.**



Third-party ICT service providers identified as “critical” may face fines of up to **EUR €5,000,000** or a maximum fine of **EUR €500,000 for an individual.**



Violations may also mean the possibility of an audit or even **suspension of a company’s operations.**

ACTION 1: ESTABLISH A COMPREHENSIVE AND WELL-DOCUMENTED ICT RISK MANAGEMENT FRAMEWORK

While most financial firms already maintain guidelines to govern their cybersecurity resilience, DORA will require firms to address ICT risks quickly, efficiently, and comprehensively to ensure a high level of digital operational resilience.



Within this framework, firms must also document:

- The rules to protect the availability, authenticity, integrity, and confidentiality of assets and data in an Information Security Policy.
- Access Restriction Policies based on functions, roles, and missions.
- Risk-based assessments of software, hardware, firmware components, systems, or security parameters as part of an ICT Change Management Policy.
- Documentation for patches and updates.

Firms have a requirement to protect both their “information assets” and “ICT assets” from risks, including damage and unauthorized access or usage. Essentially, this covers software, physical assets (hardware, software, and servers), and physical infrastructure (premises, data centers, and areas that have been designated as sensitive) with strategies, policies, procedures, ICT protocols, and tools.



The DORA regulations also stipulate that an ICT risk management framework needs to be updated:

- At least once a year.
- After an ICT-related incident.
- Following supervisory instruction.
- After resilience testing or auditing.
- The framework will also be subject to internal audit by auditors on a regular basis.



HOW CAN ECI ASSIST YOU?

We utilize frameworks that encase industry best practice. This includes, but is not limited to, Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) Cybersecurity Frameworks.

These frameworks ensure that firms can protect against cyber attacks and interruption to operations. We then conduct an assessment to determine where the gaps are and develop a comprehensive roadmap to remediate any gaps and maintain compliance.

MANAGING THIRD-PARTY RISK

Firms need a complete understanding of outsourced relationships and where their data is stored.

Businesses with contractual obligations in place for the use of ICT services to run their operations remain fully responsible for their regulatory compliance. With this in mind, DORA stipulates (5.28) that managing third-party risk is an integral part of an ICT risk management framework.³

Firms are required to adopt, and regularly review, a strategy on third-party risk that takes into account the nature, scale, complexity, and importance of ICT-related dependencies. This includes policies that document the risks that arise from the contractual agreements on the use of third-party ICT services and the potential impact on the continuity of services and activities.

Therefore, DORA requires that firms must conduct an assessment for potential third-party ICT service providers that:



Assess whether the service supports a critical or important function.



Identify and assess all relevant risks in relation to the contractual arrangement.



Undertake due diligence to ensure the suitability of the provider.



Identify and assess conflicts of interest.



Establish an appropriate exit strategy.



HOW CAN ECI ASSIST YOU?

Our GRC offering includes third-party risk management. By capturing all third-party vendors and services that a firm uses to conduct its operations, this helps understand and rate those vendors through a business impact analysis.

We review vendors through a due diligence process including questionnaires and compliance reports and report any actions that should be taken to mitigate operational and security risk.

³DORA.com

ADOPTING THE THREE LINES OF DEFENSE MODEL

In a dynamic risk landscape, firms need to be able to identify and respond to cyber threats in a quick and effective way. While the Three Lines of Defense (3LoD) model is a well-established approach to risk management, the DORA guidelines (6.4) require 3LoD so that firms have “appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions”.

As a refresher, the 3LoD model requires different groups within an organization to play a distinct risk governance role. The three lines comprise:

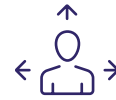


First Line of Defense (teams on the ground):

These are the operational teams directly involved in risk management. They must clearly define the responsibilities of each person and embed a culture of cybersecurity by design principles in their processes.



**Second Line of Defense
(risk and compliance teams, CISO):** This layer is responsible for monitoring and implementing a firm's overall risk management strategy and ensuring all company functions work in accordance with risk management policies.



Third Line of Defense (Independent internal auditors):

This line provides objective and independence assurance. These auditors are responsible for verifying the effectiveness of the first two lines of defense, verifying the processes and their correct execution to regulators and external auditors.

ACTION 2: DEFINE A DIGITAL OPERATIONAL RESILIENCE STRATEGY

After establishing your ICT risk management framework, financial firms will need to complement it with a digital operational resilience strategy.

A best practice approach would be conducting a cyber security gap analysis to determine your firm's internal capabilities, frameworks, policies, and procedures. This assessment will indicate your current level of compliance and what is still outstanding.

A digital operational resilience strategy will be the practical strategy to demonstrate how you will achieve full compliance, specifying the methods you will put in place to address risks and how they align with your business strategy and objectives.

Its components include:



Establishing ICT risk tolerance levels in accordance with your risk appetite.



Setting clear information security objectives with measurable indicators and key risk metrics.



Outlining the ICT reference architecture and necessary changes that are needed.



Detailing the mechanisms for detecting, preventing, and protecting against ICT-related incidents.



Evidencing the effectiveness of digital operational resilience measures, based on the number of major ICT incidents reported.



Implementing resilience testing and outlining a communication strategy for ICT-related incidents.

STRATEGIES NEED TO BE CONTINUOUSLY MONITORED AND IMPROVED

The effectiveness of any digital operational resilience strategy needs to be monitored over time to take into account how risk exposure levels have evolved. An annual report to the relevant management body must capture the findings and recommendations based on these reviews.

Strategy monitoring: To track the evolution of ICT risks and analyze the frequency, type, and magnitude of incidents, particularly cyber-attacks.

Continuous improvement: To refine strategies through mandatory post-incident reviews, whether there have been any challenges initiating business continuity plans, surveillance of cyber threats, and with operational resilience testing.



HOW CAN ECI ASSIST YOU?

Through our security assessment and road mapping services, along with client meetings, we review anything we find and work together to finalize a go-forward plan for firms.

ACTION 3: PUT A BUSINESS CONTINUITY POLICY IN PLACE

DORA also mandates that firms need a comprehensive ICT business continuity policy⁴ along with a disaster recovery plan.

This policy outlines how firms will ensure the preservation of critical or important functions and how they will deliver a quick and effective response to ICT-related incidents.

A business continuity plan must include dedicated plans for each type of incident. It must document how your firm will contain and prevent further damage following an incident, including communication measures for internal teams, external stakeholders, and relevant authorities.

The policy must include:



Annual testing: Testing also needs to be conducted after significant changes to ICT systems or to crisis communication plans.



Comprehensive backup policies and procedures: With ICT capacities to ensure continuity in the instance of primary system failure. Activating a backup must not compromise data security.



Crisis communication plans for internal and external stakeholders: So major ICT-related incidents or vulnerabilities can be disclosed by a designated Crisis Communication Officer.



Accessible records of activities: With estimates of costs and losses incurred by major incidents.



An incident management process: To be integrated with your ICT business continuity policy and resilience strategy. It must include procedures for identification, categorization, and response and provide the ability to draft and design an Incident Response Plan that aligns with DORA's obligations.

HOW TO RESPOND TO INCIDENTS

Crisis communication is an integral part of a business continuity plan and is mandated by DORA. It ensures that relevant stakeholders are informed about major ICT incidents without undue delay, with communications about the incident and what mitigation measures have been taken. Crisis communication is not essential for managing customer outreach but for maintaining trust and transparency with them.

Firms must determine their specific authority based on their operational jurisdiction and scope. This may include reporting to the Computer Security Incident Response Teams (CSIRT). While some firms may have a dedicated, in-house CSIRT, those without an internal security operations center (SOC), can outsource incident management to managed cyber security service providers (MSSPs).



HOW CAN ECI ASSIST YOU?

We help clients to create business continuity and disaster recovery policies. These manage your approach to backup and restorations, as well as disaster recovery.

⁴ DORA.com

ACTION 4: MONITOR AND TEST YOUR DIGITAL OPERATIONAL RESILIENCE

Ensuring a robust cybersecurity posture requires vigilant monitoring of cyber threats and conducting thorough digital operational resilience testing.

DORA emphasizes the need for firms to have the capability to gather information on vulnerabilities and cyber threats and to monitor any technological developments.

After conducting mapping of your information system to classify your assets based on their criticality and risk level, digital operational resilience testing should be performed either in-house or by external vendors.

Technologies and methodologies to monitor and report on digital operational resilience include:



Good IT Hygiene: To ensure IT best practices are being followed, with proper implementation of multi-factor authentication (MFA), firewalls, permissions, privilege access, and for onboarding/offboarding.



Access controls: Manage who can access data based on function and credentials with tools and best-practice methodologies to authorize appropriate levels of access following authentication.



Network segmentation: Keep data separate based on its sensitivity or its value to your business continuity by segregating datacenters, cloud environments, and networks.



Threat detection and prevention: Detect and prevent threats by deploying automated tools and services. This can include security information and event management (SIEM) based on machine learning (ML) and Extended Detection and Response (XDR) for a holistic threat view and automated response.



Vulnerability management: A Vulnerability Operations Center Uncover (VOC) can perform vulnerability assessments to identify and remediate malware, backdoors, hosts communicating with botnet-infected systems, and webservices linking to malicious content.



Threat-led penetration testing: This simulates the tactics and techniques of real-life threat actors with controlled attempts to compromise cyber resilience. For those financial entities whose failure would have systemic effects, threat-led penetration testing (TLPT) is mandatory and needs to be carried out at least every three years.



Third-party risk assessment: Screen third-party suppliers and evaluate current business partners with a framework to identify the maturity of your vendor's security regimes and which areas need to be improved. DORA also stipulates that those whose services support critical functions must have documented exit strategies.



Vulnerability scans and penetration tests: Identify cyber risks and update applications with security patches (and hardware and software configurations) to protect against zero-day threats.



User training: DORA mandates comprehensive digital operational resilience training for all employees and senior management staff so they are well-versed in managing passwords, recognizing and responding to phishing attacks, and other basics of cyber hygiene.



Bug Bounty programs: For firms who develop their own software, these programs can be established to offer rewards to white hat hackers who find something wrong with their product and report the vulnerabilities.

NEED HELP TO BECOME DORA COMPLIANT?

Being able to identify, protect against, and mitigate cyber risk is imperative for financial firms.

But delivering to the requirements of the DORA regulation doesn't have to sit solely on your shoulders. With the support of an MSSP, this doesn't mean relegating responsibility – it means equipping yourselves with the tools, resources, and expertise to accelerate your adoption of the Act.

ECI IS HERE TO HELP BECAUSE:



We make compliance manageable

We turn your compliance challenges into organizational change by building a culture of compliance readiness through an actionable process of assessment, remediation, testing, and ongoing support. With our help, we actively remove the workload associated with achieving DORA compliance as a single, capable, and proven service provider.



We reinforce confidence and reduce risk

With ECI supporting your alignment with DORA compliance, we help avoid funding hold-ups, and the potential for delays, miscommunications, and avoidable errors. As a single partner, we simplify procurement and implementation of digital operational resilience and the need for separate assessment, remediation, and testing services from multiple vendors.



We help you transform compliance needs into business advantage

By leveraging ECI's transformative expertise and our entire portfolio of cyber security, digital, and cloud solutions we can enhance your day-to-day operational performance, limit your exposure to risk, remediate your cyber shortcomings, and take you beyond compliance to competitive advantage.

GOVERNANCE, RISK & COMPLIANCE: A HOLISTIC SOLUTION

GRC) services can help with DORA compliance by enhancing your ability to proactively identify, assess, and mitigate risk, ensure compliance, and safeguard your assets. With the right partner, these can be delivered without the need for others, with solutions that will enable you to maximize your operational performance.

BEST-IN-CLASS GRC SERVICE CAN INCLUDE:



Governance program management: This provides a comprehensive view across vulnerability scanners, risk assessments, security task remediation, and policies. It ensures that your firm follows defined procedures to identify, assess, and manage risks from external and internal threats.



Security and risk assessments: This enables the ongoing management of security findings. It analyzes areas such as your current cybersecurity threat readiness, any overlooked exposures in data storage that could lead to a breach, ransomware threats, attempts to commit fraudulent crimes, and any unauthorized and malicious modifications of web page content.



Risk mitigation planning:

The creation of a work plan that is tailored to your environment and IT planning, with short-, medium-, and long-term goals to manage, eliminate, or mitigate cyber risks.



Vulnerability scanning:

Weekly internal and external vulnerability scans to identify vulnerabilities and misconfigurations across endpoints, network devices, hosted applications and cloud platforms.



Information security policy suite: With a combined policy suite, this makes it easier to ensure you can meet annual updating requirements. A policy suite shows data based on what security controls really look like, rather than a futuristic state. It treats policies as “living documents”, where updates can be made to the policy to reflect changes made to your environment.



Vendor risk management: This provides the tools to assess and understand the risk your vendors have to your organization, placing them in tiers based on confidentiality, integrity, and availability.

CONCLUSION

With the finalization of DORA, financial firms have until 17 January 2025 to implement the policies, procedures, and tools that meet the requirements of digital operational resilience.

If you need a helping hand to achieve this, ECI is an expert authority to support DORA compliance. As a Managed Service Provider (MSP) and an MSSP, we can guide and enable you to drive and embed organizational change and identify and remediate internal and third-party points of failure.

With DORA principles already built into our solutions, we bring a number of proven capabilities upholding compliance standards (including SEC regulations, SOC2, ISO 27001, NIST, CSF, and NIS2).

Becoming DORA compliant and improving your digital operational resilience isn't only about regulatory need - it's also an opportunity to strengthen your critical business capabilities, enhance vendor relationships, accelerate operational performance, and improve investor confidence.

The time to begin is now.



ABOUT ECI

ECI is the leading provider of managed services, cybersecurity, and digital transformation for alternative financial services organizations across the globe. With its unmatched platform of solutions, ECI provides assured business acceleration through technology, partnering with clients to drive innovation. More than 1,000 customers worldwide with over \$3 trillion of assets under management put their trust in ECI.



READY TO BECOME MORE OPERATIONALLY RESILIENT?

Contact ECI today for assured business acceleration through technology.

+44 207 071 6802 | eci.com