

A CISO's Guide to DORA

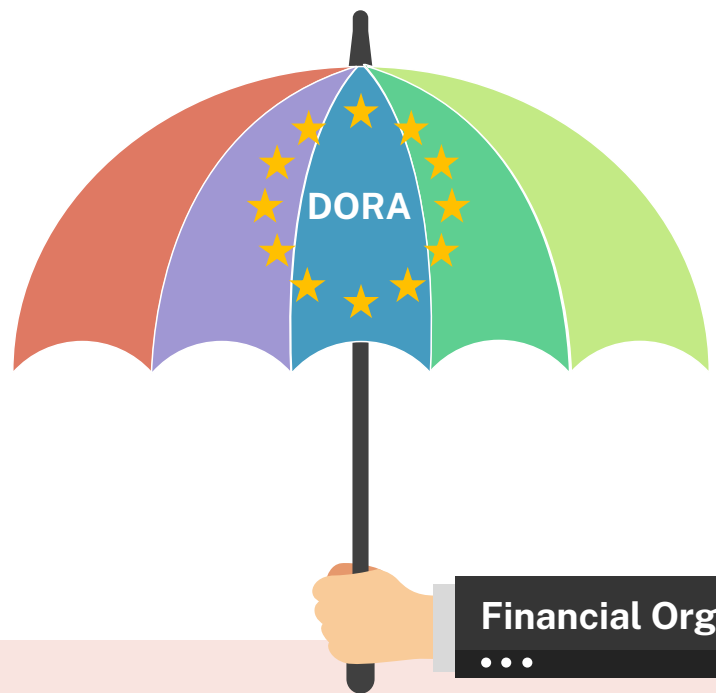




As digital transformation in the financial sector ramps up, its exposure to cyber threats is skyrocketing — moving cybersecurity to the top of the priority list in boardrooms everywhere. In the European Union, the response to these evolving challenges is [The Digital Operational Resilience Act](#) (DORA), which aims to strengthen financial entities' cybersecurity and operational resilience.

This ebook guides Chief Information Security Officers (CISOs) and CSOs as they wade through the complexities of DORA. It offers insights into its requirements, implementation strategies, and the broader impact on the EU financial sector's cybersecurity governance.

Introduction to Key Concepts



1

Materiality

This refers to the significance of an event, fact, or item. Materiality matters because it can influence decisions, affect interpretations, or change outcomes.

2

Risk Assessment/Management

This involves the identification, evaluation, and prioritization of risks, and the application of resources to minimize, control, and mitigate their impact. A business might assess the risk of a data breach and manage it by enhancing their cybersecurity measures.

3

Incident Reporting

This is the process of documenting all details of an event that could possibly result in personal injury or damage to property. For instance, if a worker is injured on a construction site, an incident report would be necessary to document what happened and why.

4

Governance

Governance refers to the structures and processes in place for managing an organization and guiding its path towards achieving its goals. An example of this could be a corporation's board of directors who set the strategic direction and oversee the management of the company.

5

Operational Resilience

This is an organization's ability to withstand, adapt to, and recover from disruptions while continuing to serve its customers or perform its critical operations. A bank, for example, may demonstrate operational resilience by ensuring it can still operate during a power cut or cyber attack.

What is operational resilience, and how do organizations measure it?

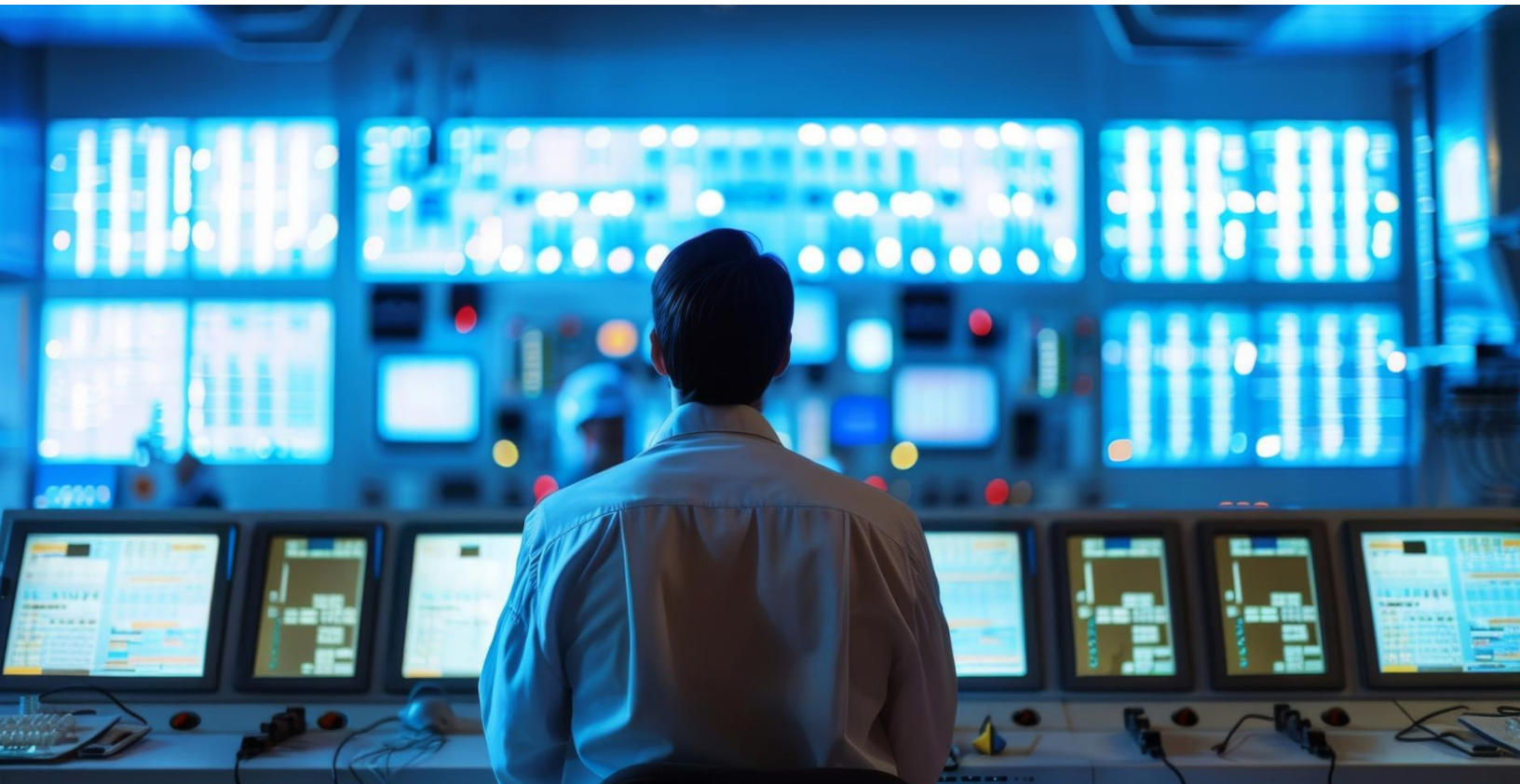
Of the 5 key concepts, Operational resilience requires some additional discussion. It refers to an organization's ability to continue providing critical operations through any disruption, such as cyberattacks, natural disasters, or system failures. It encompasses the ability to recover from incidents and anticipate, prevent, adapt to, and recover from them to minimize the impact on services, customers, and the market.

Organizations typically use a combination of metrics, such as [recovery time objectives \(RTOs\)](#), [recovery point objectives \(RPOs\)](#), and the overall time to recover critical services after an incident.

For example, scenario testing, like tabletop exercises and simulations, plays a crucial role in measuring an organization's operational resilience by testing its responses to hypothetical scenarios to identify potential weaknesses and areas for improvement.

Organizations also focus on the resilience of their supply chain and third-party vendors to effectively measure operational resilience, understanding that their operational resilience is only as strong as the weakest link in their operational chain. Key performance indicators (KPIs) related to incident response times, incidents over time, and customer feedback on service availability during disruptions can provide valuable insights into an organization's operational resilience.

Regulatory compliance metrics, especially under frameworks like DORA, ensure that financial entities meet minimum standards for resilience while striving for continuous improvement in their operational resilience capabilities.



What Does ICT mean, and what is its scope?

In the context of DORA, ICT (Information and Communication Technology) encompasses all digital technologies that facilitate the processing, storage, and transmission of information within financial entities. This broad definition includes traditional IT systems, cloud computing services, networks, and digital platforms that support financial operations, data analytics, and customer interactions.

The scope of ICT in DORA is deliberately broad in that it covers the extensive range of technologies used by financial entities, reflecting the diverse and evolving nature of the digital landscape in the financial sector. DORA's comprehensive approach ensures that all aspects of ICT that could impact the operational resilience of financial entities are addressed.

The scope of ICT under DORA also extends to the management of third-party risks, recognizing the significant reliance of financial entities on external ICT service providers. This may include cloud services, data processing, and cybersecurity solutions. By including these third-party services, DORA aims to ensure a holistic approach to operational resilience. It requires financial entities to assess, monitor, and mitigate risks within their ICT infrastructure and across their extended digital ecosystem.

Through this broad and inclusive approach, DORA seeks to enhance the overall resilience of the EU financial sector against a wide array of ICT risks, ensuring stability and trust within the industry.

The Vital Role of Cybersecurity Governance in the EU Financial Sector

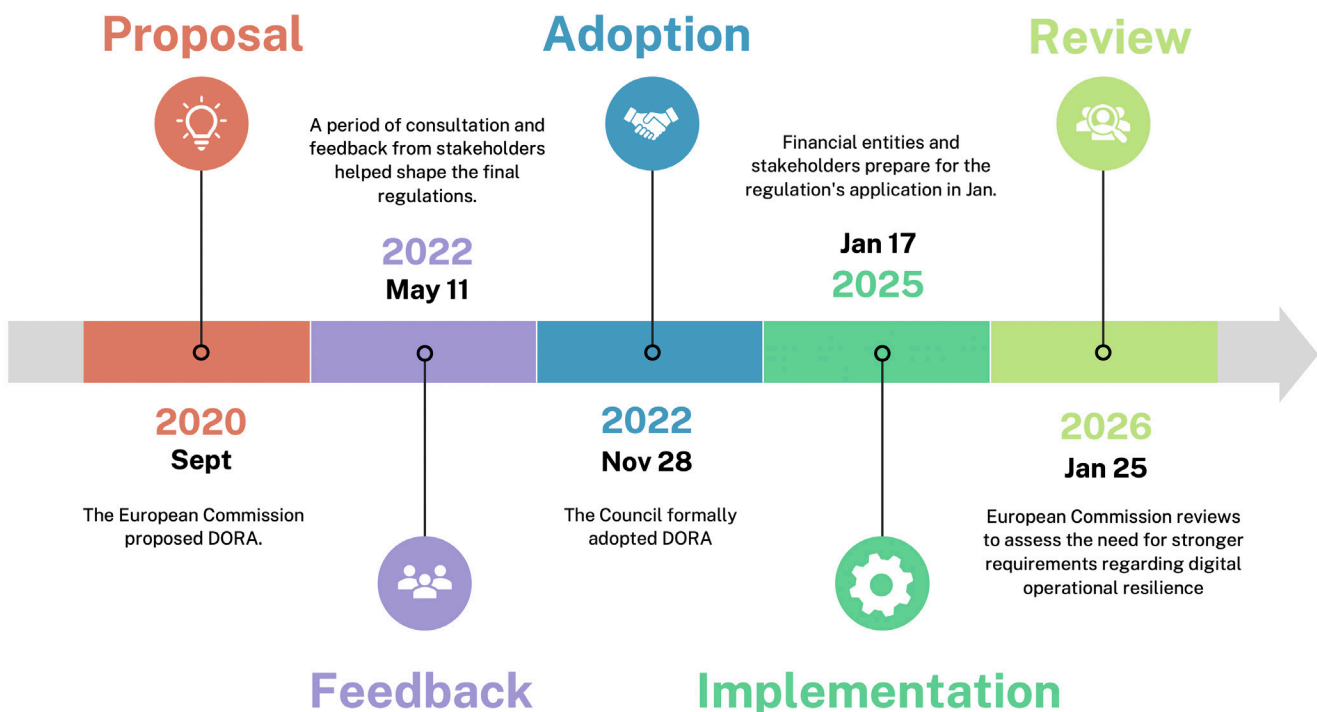
The goal of cybersecurity governance in the EU financial sector is to protect information and systems from cyber threats and ensure the stability and integrity of the financial markets.

Effective cybersecurity governance under DORA involves a holistic approach, encompassing risk management, regulatory compliance, incident response, and resilience planning. Most importantly, it requires leadership from the C-suite, with CISOs playing a crucial role in aligning cybersecurity strategies with business objectives and regulatory requirements.

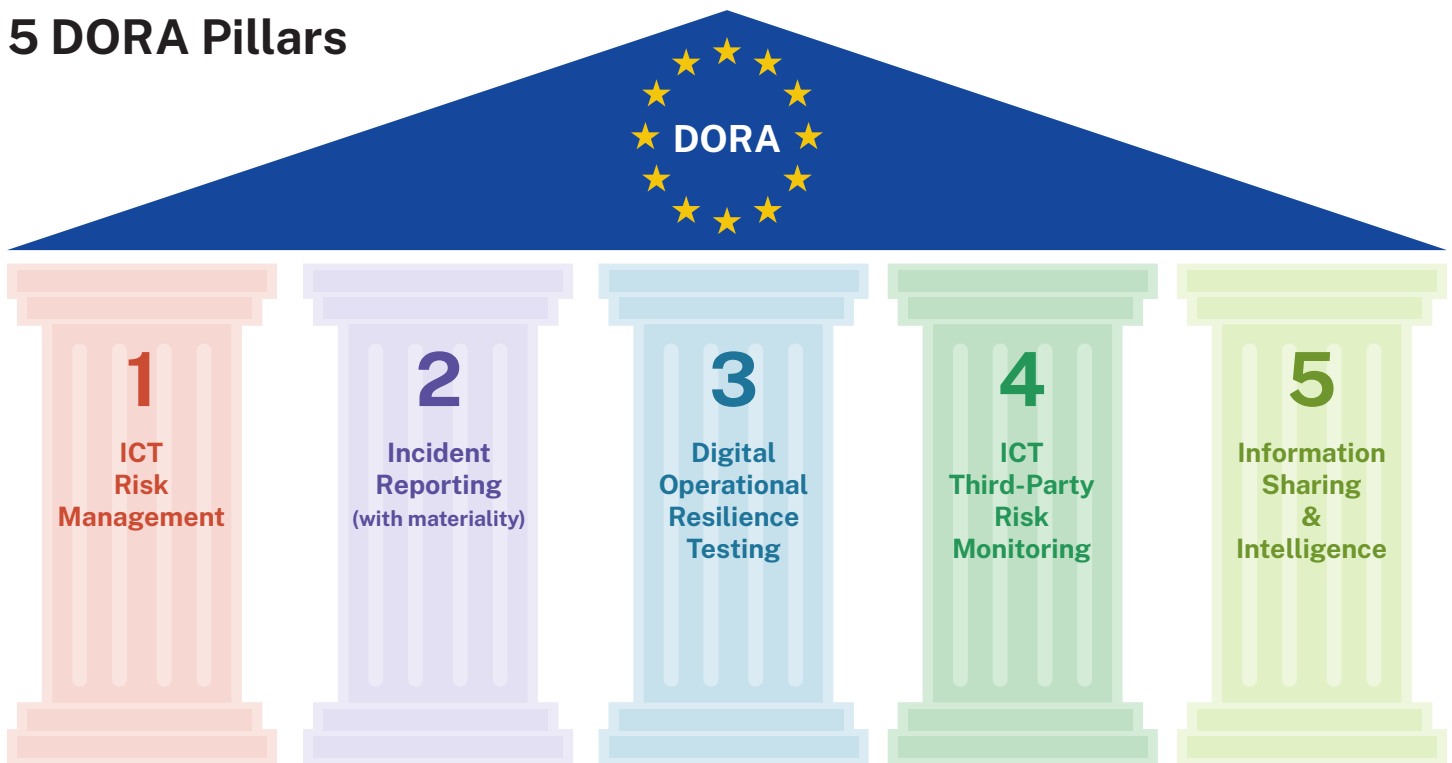
What you need to know about **DORA**

Timeline of the Development and Adoption of European DORA Cybersecurity Regulations

Several key milestones have marked the development and adoption of DORA:



5 DORA Pillars



1 ICT Risk Management

ICT Risk Management under DORA requires financial entities to establish and maintain a comprehensive risk management frameworks. These frameworks should be capable of identifying, assessing, mitigating, and managing ICT risks that could impact the entity's operational resilience.

The key elements of ICT Risk Management you need to know about are →

Risk Assessment — Regularly conduct risk assessments to identify vulnerabilities within the ICT systems and processes. Though not specified in the regulations, frequency should be appropriate to the nature, scale, and complexity of the risks faced by a particular business.

Policies and Procedures — Developing and implementing policies addressing identified risks.

Protection and Prevention — Implementing protective measures and controls to prevent ICT-related incidents and to minimize their impact on critical functions.

Incident Response and Recovery Plans — Establishing incident response and recovery plans to ensure the entity can quickly respond to and recover from ICT disruptions or incidents.

2 Incident Reporting

Incident Reporting mandates that financial entities promptly report significant cybersecurity incidents to relevant authorities, typically within 72 hours. This component is crucial for maintaining transparency and enabling regulatory bodies to monitor systemic risks that could affect the financial sector's stability.

Key aspects of incident reporting include →

Reporting Thresholds — Defining thresholds for incident reporting based on the incident's impact on the entity's operational capabilities, the financial interests of clients, and the financial market's integrity.

Timely Notification — Ensuring incidents are reported within a tight timeframe (typically 72 hours) to allow for an adequate regulatory response.

Detailed Reporting — Providing comprehensive details about the incident, including the type, impact, vulnerabilities exploited, and measures taken or planned for mitigation and recovery.



Digital Operational Resilience Testing

Digital Operational Resilience Testing requires entities to regularly test their ICT systems and processes to ensure they can withstand and recover from operational disruptions.

This proactive approach to resilience includes →

Penetration Testing — Conducting penetration tests to identify vulnerabilities in ICT systems and networks.

Scenario-Based Testing — Implementing scenario-based testing assesses the entity's preparedness and response mechanisms against various ICT disruptions.

Testing Frequency and Rigor — Ensuring testing is conducted at a frequency and rigor applicable to the entity's size, complexity, and risk profile.



ICT Third-Party Risk Monitoring

ICT Third-Party Risk Monitoring highlights the importance of overseeing and managing risks associated with third-party ICT service providers.

Given the increasing reliance on third parties for critical ICT services, DORA requires →

Due Diligence — Performing due diligence before entering into agreements with third-party providers to ensure they meet security and resilience standards.

Contractual Agreements — Include provisions in contracts that allow for the monitoring, auditing, and testing of the third party's services.

Ongoing Monitoring — Continuously monitoring the performance and compliance of third-party providers with respect to ICT risk management and security requirements.



Information Sharing and Intelligence

Information Sharing and Intelligence encourages financial entities to share information about cyber threats, vulnerabilities, incidents, and best practices.

This collaborative approach aims to enhance the collective operational resilience of the financial sector by →

Establishing Information-Sharing Arrangements — Participating in information-sharing platforms or arrangements with peers, relevant authorities, and cybersecurity organizations.

Protecting Shared Information — Ensuring that shared information is protected appropriately to maintain participant confidentiality and trust.

Leveraging Intelligence — Using shared information to improve the entity's own cybersecurity posture and resilience strategies.

DORA's comprehensive approach, covering these core components, was crafted to standardize and elevate the cybersecurity and operational resilience practices across the EU's financial sector.



Scope and Applicability

Why such a broad scope?

The Digital Operational Resilience Act (DORA) encompasses a wide range of financial entities and critical third parties to address the intricacies of the modern financial ecosystem, which is deeply interconnected and reliant on many ICT services. By ensuring comprehensive coverage, DORA aims to safeguard the financial sector against potential vulnerabilities, whether they originate within traditional banking institutions, innovative fintech startups, or the third-party service providers that support them.

Advantages of compliance

Compliance with DORA offers the EU financial sector uniform standards of operational resilience, enhancing stability and consumer protection across the board. This uniformity not only levels the playing field among financial entities of all sizes but also addresses systemic risks more effectively, ensuring the entire ecosystem is resilient to ICT risks.

Regulatory Cooperation and Oversight




DORA fosters a cooperative framework among EU and national regulatory authorities to harmonize the application of its provisions, ensuring consistent operational resilience across the financial sector. The framework includes sharing information on cyber threats, coordinating supervisory activities, and executing enforcement actions to address compliance challenges.

DORA also introduces oversight for critical third-party ICT service providers, requiring rigorous assessment and monitoring to protect the financial ecosystem's integrity.



A DORA Compliance Checklist

The following is a checklist of requirements for DORA compliance:



Reporting Cybersecurity Incidents

-  **Timely Incident Reporting Obligations** — Financial entities must report significant cybersecurity incidents to relevant authorities promptly while adhering to DORA's strict timelines.
-  **Materiality Assessment Criteria** — Entities must assess the materiality of incidents based on their impact on operational capabilities and financial stability, guiding reporting decisions.
-  **Reporting in Cases of Information Unavailability** — In situations where all relevant information about an incident is not immediately available, entities must still report in a timely manner, providing updates as any new details become available.

Cyber Risk Management and Strategy

-  **Risk Identification and Mitigation Processes** — Entities must continuously identify ICT risks and implement effective mitigation strategies to protect against potential threats to operational resilience.
-  **Integration of Cyber Risks with Business Strategy** — Cyber risk management processes should be fully integrated into the entity's overall business strategy, ensuring that cybersecurity considerations are key to organizational decision-making.

Cyber Governance

-  **Board of Directors Oversight** — The board oversees the entity's cybersecurity posture, ensuring that cyber risk management is aligned with strategic objectives and regulatory requirements.
-  **Management's Role and Expertise in Risk Assessment and Policy Implementation** — Senior management must demonstrate expertise in risk assessment and implementing cybersecurity policies. They must play a key role in fostering a culture of cyber resilience.
















Preparing for DORA Compliance

Preparing for DORA compliance involves actionable steps. Here are five to get you started:



How Balbix can help

The Balbix AI-powered Cyber Risk Platform improves operational resilience against the backdrop of evolving threats, enabling compliance with all five key pillars of DORA requirements:

DORA Requirements		How Balbix Helps
 ICT Risk Management		 Balbix provides visibility into all assets & vulnerabilities, facilitating prioritization based on risk, & quantifying potential impact.
 Incident Reporting		 Balbix helps facilitate materiality determination for incident reporting.
 Digital Operational Resilience Testing		 Balbix continuously monitors and assesses vulnerabilities as well as misconfigurations and security controls.
 ICT Third Party Risk Monitoring		 Balbix can integrate with dozens of tools to provide visibility into risks.
 Information Sharing		 Balbix uses threat intelligence to determine how to prioritize cyber risks & vulnerabilities, though it doesn't currently have an info sharing capability.

About Balbix

Balbix enables businesses to rapidly reduce cyber risk by identifying and mitigating their riskiest cybersecurity issues. Balbix ingests data from hundreds of security and IT tools to deliver actionable insights for risk reduction. With Balbix, businesses get asset inventory, risk-based vulnerability management and cyber risk quantification in a single platform. Balbix was recognized in Forbes America's Best Startup Employers 2024 and ranked #32 on the 2021 Deloitte Fast 500 North America.



Request a [demo](#) to learn more about how Balbix helps CISOs prioritize cyber risk.

