HOUSE OF
CONTROL

DORA Guide:

What you need to know about **EU's Digital Operational Resilience Act**

HOUSE OF
CONTROL

Table of Contents

HOUSE OF CONTROL

DORA is a significant step forward in regulating digital operational resilience in the financial sector. It provides a clear framework for managing digital risks and establishes practical steps that organizations must follow.

To comply with DORA takes careful planning, effective implementation, and a commitment to continuous improvement. If done correctly, financial institutions can secure a safer, more robust future for themselves and the financial system as a whole.

Disclaimer: *At House of Control, we help our clients navigate DORA requirements regarding third-party ICT risks. Our effective and practical solution is a digital register for all third-party ICT service providers, as mandated by DORA Article 28 (3). It has been developed together with one of the largest finance institutions in the Nordics to help our clients in its work with complying with the DORA requirements.*

House of Control is a software company. We do not offer DORA compliance consulting services. Thus, ***following these advice does not guarantee compliance with all DORA legal requirements****. The contents of this guide are based on our own research of the DORA requirements, and includes inspiration from various actors offering compliance services. We do not assume any responsibility or liability for any failure to comply with DORA requirements or resulting from the use of this guide.*

Introduction

DORA is a new EU law that came into force in January 2025. Its goal is to strengthen digital operational resilience in the financial sector. The law sets out clear requirements for managing digital risks, handling incidents, testing system resilience, overseeing third-party providers, and sharing important information.

It applies to a wide range of financial institutions such as banks, insurance companies, payment service providers, investment firms, and crypto-asset service providers. For companies that need to meet these requirements, especially in the area of managing risks related to external technology providers, effective software solutions can be a key part of the strategy.

This guide explains the core concepts of DORA, with a special focus on third-party risk management and how software tools can help organizations stay compliant.

Core principles of DORA

DORA is built on several core principles that work together to safeguard the financial sector. At its heart, the law requires that companies are well prepared to manage digital risks. This includes having robust plans for risk prevention, immediate and effective response when incidents occur, and rapid recovery afterward.

The regulation demands that finance firms develop clear frameworks for managing digital risks, continuously monitor their systems, test their resilience under realistic conditions, and carefully manage the risks that come from using external service providers. In addition, DORA encourages the sharing of information about emerging digital threats among financial institutions so that the entire sector can learn from each other's experiences and improve their defenses.

Impact on financial stability and resilience

DORA has significant implications for the stability of the financial system. Digital failures or successful cyberattacks on a single institution can have ripple effects that threaten the broader market. By establishing strict standards for risk management and incident response, DORA helps to minimize the impact of such events. Financial institutions that comply with DORA are better prepared to detect, respond to, and recover from digital disruptions. This not only limits the potential damage but also helps restore normal operations more quickly, contributing to overall financial stability.

A robust digital resilience framework enhances customer confidence. When customers are assured that their financial service provider has strong systems in place to manage and mitigate digital risks, they are more likely to trust that institution with their financial needs. Although the initial investments required to meet DORA's standards can be substantial, the long-term benefits of a more secure and resilient financial environment far outweigh these costs. Ultimately, a well-implemented DORA framework contributes to a more stable, reliable, and trustworthy financial system.

ICT risk management

Managing risks related to information and communication technology is the foundation of DORA. Every financial institution is required to develop a comprehensive framework for ICT risk management that is approved by the board of directors. This framework must clearly define roles and responsibilities, set appropriate risk tolerance levels, and allocate sufficient resources to monitor and manage digital risks.

Organizations are expected to create written plans that detail all digital assets and the risks associated with them, and these plans must be kept up to date as the technological landscape evolves.

Regular training for employees is essential so that everyone understands how to identify potential risks and what actions to take when unusual events occur. In addition, firms should invest in tools that quickly detect any abnormal activity, ensuring that incidents can be identified and managed promptly.

Regular reporting to senior management helps maintain focus on digital risks and ensures that any changes in the risk profile are addressed as soon as possible.

Incident management

Even the best-prepared systems can experience failures or cyberattacks, which is why DORA requires a clear process for incident management. Organizations must establish systems that detect problems early, record every incident in detail, and analyze the causes behind them.

Each incident should be documented with information about when it occurred, what its impact was, and what measures were taken to resolve it. This careful logging and analysis allow organizations to identify the root causes of incidents so that similar problems can be prevented in the future.

When a significant incident occurs, it is essential that the organization communicates with the relevant regulatory authorities in a timely manner. Effective communication, both internally among staff and externally with clients and regulators, is a critical element of incident management. By maintaining clear procedures and ensuring that staff are well trained, firms can minimize the damage caused by any digital incident and learn from each experience.

Resilience testing

Regular testing of digital systems is a key requirement under DORA. Organizations must conduct resilience tests to determine how well their systems perform under stress and to identify any vulnerabilities that could be exploited by cyberattacks. These tests are designed to mimic real-world scenarios, including simulated cyberattacks known as threat-led penetration testing.

Such tests help firms understand how their systems would behave during an actual incident and whether their response procedures are effective. Testing must be performed on all critical systems, whether they are managed internally or provided by third-party vendors. The results of these tests should be carefully analyzed so that any weaknesses or deficiencies are quickly addressed.

In some cases, independent experts may be engaged to carry out the tests to ensure an unbiased evaluation. Through continuous testing and subsequent improvements, financial institutions can build a robust system that stands up well against digital threats.

Third-party risk management

A significant focus of DORA is on managing the risks associated with external ICT providers. Many financial institutions rely on third-party vendors for critical services, and ensuring these relationships are secure is essential for overall operational resilience. Here are the the steps your organisation can take to ensure compliance:

1. Maintain a comprehensive vendor register: Organizations must maintain a comprehensive register that lists all external ICT providers along with detailed information about the services they deliver and the level of risk each service represents.

2: Conduct thorough assessments before contracting: Before entering into any contract with a third-party provider, a thorough assessment of the provider's security standards is required. Clear contractual obligations must be established that define the responsibilities of both parties with regard to digital security and continuity.

3. Perform ongoing monitoring and evaluation: Once a contract is in place, ongoing oversight is necessary to ensure that the provider continues to meet the required standards. Regular audits, performance evaluations, and pre-defined exit strategies are important elements of this oversight.

4. Leverage technology to streamline the process: For organizations looking to simplify and streamline this process, specialized software solutions offer significant benefits. Software designed to manage third-party risk can automate the creation and maintenance of a detailed provider register, send timely alerts when contracts are due for renewal or when compliance issues are detected, and integrate smoothly with existing risk management systems.

5. Enhance risk management and response: By centralizing information about all external ICT providers, these tools help organizations reduce administrative burden and maintain an up-to-date overview of the risks associated with each provider.

This not only supports compliance with DORA but also enhances the organization’s ability to respond quickly if an issue arises with a particular vendor.

Information sharing

DORA recognizes that no institution is completely isolated from digital threats. The law encourages financial institutions to share information about cyber threats and vulnerabilities with one another. By exchanging relevant data on potential risks and actual incidents, organizations can benefit from the collective experience of the sector. This collaborative approach enables faster detection of widespread threats and more effective responses to emerging issues.

Information sharing should occur within trusted networks that ensure the confidentiality of sensitive data and comply with legal and regulatory requirements. When institutions actively share insights and lessons learned, the entire financial ecosystem becomes better prepared to face new and evolving cyber threats. This spirit of cooperation is vital for maintaining the overall security and resilience of the financial sector.

Steps to DORA compliance

1. Conduct a gap analysis to identify compliance shortcomings: Achieving compliance with DORA is a structured process that begins with a thorough review of current practices. The first step is to conduct a comprehensive gap analysis in which the organization compares its existing digital risk management practices with the specific requirements laid out in DORA. This analysis helps to identify any shortcomings or areas that need improvement.

2. Develop a detailed roadmap for compliance: Once the gaps are clearly defined, a detailed roadmap should be developed that outlines the tasks, priorities, and deadlines necessary to bring the organization into full compliance. This roadmap must cover all aspects of DORA, including ICT risk management, incident handling, resilience testing, third-party risk oversight, and information sharing.

3. Update and formalize the ICT risk management framework: After completing the gap analysis, companies need to update or create their ICT risk management framework. This involves writing a clear and detailed plan that specifies how digital risks will be managed, how incidents will be detected and reported, and how third-party providers will be assessed. It is essential that this framework receives approval from the board of directors and is integrated into the overall risk management strategy.

4. Invest in technology to enhance monitoring and automation: Investment in the appropriate technology is crucial. Firms must implement monitoring tools that can automatically detect unusual activity and help log incidents, while software solutions that handle third-party risk can ease the administrative burden. Automating parts of the reporting process can also streamline compliance efforts.

5. Ensure staff training and awareness: Training plays an important role in ensuring DORA compliance. Every employee, from frontline staff to senior management, should be made aware of the new procedures and understand their individual responsibilities. Regular training sessions and workshops help reinforce these responsibilities and keep everyone updated on any changes to the process.

6. Establish continuous monitoring and periodic reviews: Finally, it is important to establish continuous monitoring and periodic reviews. This means that risk assessments, system tests, and third-party evaluations should be conducted on an ongoing basis, with updates made to the framework as new threats emerge. By committing to continuous improvement, organizations can ensure that they remain compliant and resilient over time.

Common challenges and how to overcome them

Implementing the requirements of DORA can be complex, especially for institutions that must overhaul long-established practices. One common challenge is integrating new digital risk management requirements into existing systems without causing disruptions to day-to-day operations. A thorough gap analysis can help identify these issues and prioritize the areas that require immediate attention.

Managing the large number of third-party providers is another significant challenge. Many financial institutions work with a diverse range of external ICT vendors, each of which may have different security standards and operational practices. Maintaining a comprehensive, up-to-date register of these providers and standardizing the assessment process can simplify oversight and reduce complexity. Software solutions that automate these processes can be particularly helpful in reducing administrative burden and ensuring consistency.

Resource constraints, especially for smaller firms, also present a challenge. The costs associated with upgrading technology, training staff, and conducting regular tests can be high. Prioritizing high-risk areas and leveraging automation can help mitigate these costs.

Finally, ensuring that the board of directors and senior management are fully engaged in the compliance process is crucial. Clear, concise reports and dashboards that highlight key performance indicators can help maintain their focus on digital risks. Regular updates and targeted training for senior management can foster better understanding and support for the compliance process.

Conclusion

Although the process of achieving compliance with DORA can be challenging and may require significant investment in technology, training, and process improvement, the long-term benefits are considerable. Organizations that implement the necessary changes not only comply with the law but also build a stronger, more resilient foundation for their operations and improve customer confidence.

Achieving DORA compliance is an ongoing journey that begins with a thorough evaluation of current practices and ends with continuous improvement and adaptation to emerging threats. By working together, investing in the right tools, and maintaining clear communication at all levels of the organization, firms can create a secure environment that meets the challenges of the digital age.

HOUSE OF CONTROL

Thank you for your interest in **House of Control!**

Read more about our DORA solution:

DORA software

Contact

House of Control AS
O.H. Bangs vei 70 1363 Høvik, Norway
+47 815 66 355

www.houseofcontrol.com
mops@houseofcontrol.com
Follow us: Linkedin