IM_

DORA

The EU Digital Operational Resilience Act

Table of contents

1. Introduction to the EU Digital Operational Resilience Act

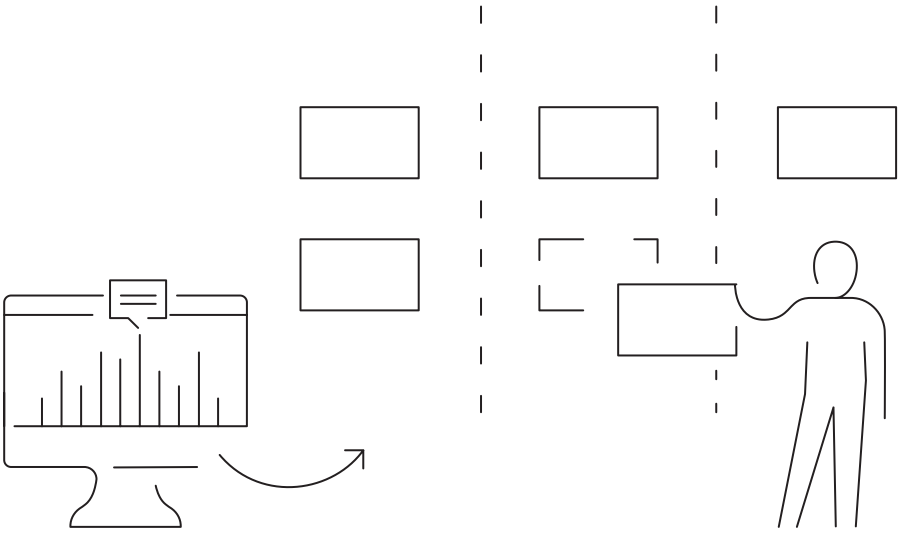
Welcome to a practical guide to navigating the Digital Operational Resilience Act (DORA) – a key EU regulation designed to strengthen digital resilience in the financial sector.

DORA introduces directly applicable rules for Member States, which means that it enters into force without additional national legislation – also here in Denmark.

The goal of DORA is critical: To ensure a robust and resilient society by ensuring that financial institutions are fully equipped to withstand, respond to and quickly recover from cyberattacks and technology failures. This is achieved through five core areas or "pillars" that include IT security governance, IT incident management, digital resilience testing, third-party risk management and information sharing.

In order to strengthen the resilience of the sector and thereby protect clients and, ultimately, society, it is crucial that we understand the roles in connection with implementing DORA. This guide offers a step-by-step introduction to the key principles and requirements of DORA and how to meet those requirements.

Let us dive into what DORA means and how we can ensure that the financial service organisations and the financial sector not only comply with but excel in digital operational resilience.



2. What is digital resilience?

The regulation focuses on the ability of financial institutions to withstand and overcome technological threats.

DORA requires financial institutions to:

- Identify and document key information and communication technologies (ICT) and services that may affect their operation.

- Assess risks associated with these technologies and services and implement measures to mitigate these risks.

- Build robust cyber defence measures to protect against cyber threats.

- Establish effective incident reporting systems to quickly respond to and recover from IT security incidents.

- Conduct regular tests of digital resilience, including testing capacity to withstand cyberattacks.

The purpose of DORA is to ensure that the financial sector can continue to operate efficiently and securely, even in the event of technological failures or cyberattacks, thus protecting society, institutions and their clients. For practitioners in the banking sector, this means that there must be a continuous and systematic approach to improving and maintaining digital resilience.

3. The five pillars: The main elements of DORA

DORA introduces five main elements/pillars that together form the backbone of digital resilience regulation for the financial sector. Understanding these pillars and how they are operationalised is essential for banking practitioners who are faced with implementing the new requirements.

3.1. IT security management

The focus is on developing a robust framework to protect critical IT systems and data from cyberattacks and other security threats. This involves identifying and securing the organisation's most valuable assets.

3.2. Significant IT incidents

This area covers the process of effectively handling and reporting major IT incidents to the relevant authorities. A quick and effective response is necessary to minimise damage and learn from these incidents.

3.3. Digital operational resilience test

Financial service organisations must regularly test their ability to withstand and recover from digital attacks and failures. This involves both internal audits and external tests performed by approved third parties.

3.4. Third-party risks

As financial service organisations often rely on third-party vendors for critical IT services, they must also ensure that these partners meet strict security standards. This requires due diligence and continuous monitoring of third-party vendors.

3.5. Information sharing

To strengthen the resilience of the entire sector, DORA recommends secure sharing of threat knowledge and best practices between financial institutions.

By understanding and implementing these five pillars, we ensure that our clients remain resilient to digital threats, protect their clients' assets and support overall financial stability.

4. DORA in practice: Implementing basic principles

Implementing DORA requires a clear and focused effort from the entire organisation.

Here is a short guide on how we ensure the integration of the DORA principles into strategies, policies, training and communication.

Policies and strategy

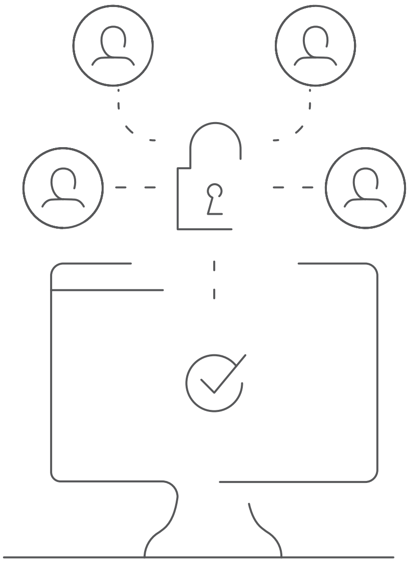
- We ensure policy updates: We ensure that our policies clearly reflect the principles of DORA regarding IT security and risk management. They must be easy to understand and accessible to all employees.

- We integrate the principles into our business strategy: Digital resilience is an integral part of the financial sector's overall strategy and risk management. We secure roles and responsibilities under the five pillars and ensure that client practices comply with the requirements of DORA.

Education and communication

- We raise awareness through education: We offer and regularly conduct training programmes to increase employees' understanding of cybersecurity and the specific steps needed to comply with DORA.

- We ensure effective information: We offer and use tailored communication strategies, including courses and online training, to effectively share knowledge about DORA-related topics both internally at Implement and with our clients and partners.



Implementation at a glance

By focusing on the key areas – updating policies, integrating the principles into the business strategy, training employees and effective communication – we ensure the successful implementation of DORA. This approach confirms our commitment to digital resilience and regulatory compliance.

5. Operationalising the five pillars

Each of the five pillars of DORA must be handled in its own way. Only through correct and continuous operationalisation of the five pillars can the necessary resilience be created for the financial sector and its clients.

5.1. Operationalisation of IT security management

To strengthen the digital operational resilience of the financial sector, DORA places a strong emphasis on establishing and maintaining robust IT security management policies and procedures. These must include:

- **Purpose and scope:** All employees should understand that the IT security strategy is designed to protect both the organisation's data and internal IT infrastructure from cyberattacks and other digital threats. It is the foundation of our overall digital health.

- **Governance and policies:** Management is dedicated to promoting a culture of security. This includes clear guidelines on who is responsible for what in IT security and how those responsibilities are managed.

- **Process and requirements:** Implementing effective security practices is not a one-time undertaking but an ongoing process. This includes regular policy updates, risk assessments and security audits to ensure that our clients stay ahead of potential threats.

5.2. Operationalising the management of significant IT incidents

It is crucial that all employees are trained to identify, report and manage significant IT incidents. DORA requires that employees in the financial sector:

- **Identify:** Are aware of and report any suspicious activities or vulnerabilities that could indicate a security incident.

- **Report:** Have established clear channels for quick and efficient reporting of potential threats so that the IT security team can respond immediately.

- **Handle:** The IT security incident response plan includes emergency procedures, communication strategies and recovery plans to minimise the damage of any security breaches.

5.3. Operationalising organisational resilience testing

Regular testing of the client's digital resilience is essential. This includes:

- **Test planning:** We offer and conduct regular penetration tests, simulated attacks and recovery tests to evaluate defence and recovery procedures.

- **Implementation and follow-up:** After each test, we offer an analysis of the results to identify and address any weaknesses. This ensures continuous improvement and adaptation to new threats.

5.4. Operationalisation of working with third parties, risks and responsibilities

The organisation's collaboration with third-party providers and suppliers must be even better secured under DORA:

- **Risk management:** We offer an assessment of security practices and policies to ensure that they meet the extended requirements of DORA and best practice standards.

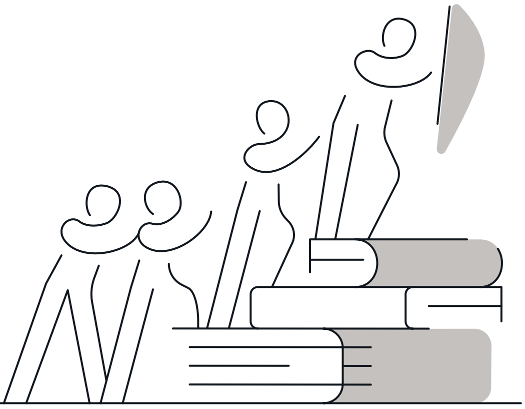
- **Responsibility and monitoring:** We provide guidance and set clear requirements and responsibilities in clients' contracts with third parties and offer to perform regular audits to monitor compliance.

5.5. Operationalisation of information sharing under DORA

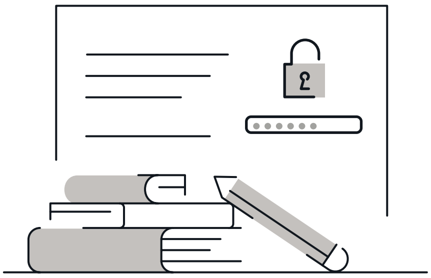
Sharing information about cyber threats and IT security incidents with relevant parties, including NFCERT and other financial institutions, is essential:

- **Collaboration:** By sharing information and best practices across the financial sector, together we can strengthen the sector's defences against digital threats.

- **Communication channels:** We provide guidance on maintaining active lines of communication with relevant organisations for the effective exchange of important security information.



6. Get guidance from EU regulators



The European Supervisory Authorities for banking, pension and insurance, also known as ESA, have been tasked with guiding the sector on the requirements of DORA. They have done this in so-called delegated acts, which translate into "Regulatory Technical Standards (RTS)". These are a series of standards under the regulation itself that are intended to support and specify requirements and expectations. The technical standards play a key role in operationalising DORA by providing detailed guidance and setting out specific minimum requirements.

Understanding and applying RTS is key to compliance. Here is a simple guide:

- **Overview and responsibilities:** Map the RTS principles against the five pillars. This ensures that you know exactly which areas require attention and action when we know the maturity level. We (Implement) have done this mapping and offer this as an accelerator.

- **Updated practices:** Update policies and procedures based on the guidance from the RTS principles to ensure full compliance. We (Implement) have prepared practical examples of how and where to update effectively.

- **Training and information:** Provide ongoing training of all employees on changes relevant to them to promote a strong compliance and security culture. We (Implement) have prepared template training programmes as inspiration.

By following these steps, you can effectively navigate the complex requirements and ensure that your organisation is fully compliant with DORA.

7. Help the client get started: Step by step

Here is a step-by-step action plan to help financial practitioners in the process of effectively implementing DORA.

Identify your "pillar responsibilities"

- DORA is based on five main pillars (described in section 4): IT security management, Significant IT incidents, Digital operational resilience test, Third-party risks and Information sharing. First, identify which pillar(s) your role and specialist knowledge/responsibilities relate to.

Find the area of responsibility

- Once you have identified the pillar(s), the area of responsibility needs to be precisely defined. This includes understanding how we contribute to strengthening the digital resilience of the organisation within the pillar(s) in question.

Knowledge of requirements

- For each pillar, understand the specific requirements set by DORA. This includes everything from policies and procedures to specific technology solutions that support digital resilience.

Seek guidance and advice

- The Regulatory Technical Standards (RTS, described in section 7) provide detailed guidance on how to meet the requirements of DORA. Review those that relate to the relevant area to understand what is specifically expected of them.

- If you have any doubts or need further guidance, do not hesitate to contact the DORA team at Implement. We are ready to offer advice and support in all aspects of the implementation of DORA. You can find our contact information at the end of this leaflet.

Implementation and compliance

- With clear communication of responsibilities and requirements under DORA, develop and implement measures to ensure compliance.

- DORA is not a one-time task but an ongoing process. Be proactive in guiding ongoing monitoring, reporting and improvement of processes and systems to ensure continued compliance with the requirements of DORA.

By following these steps, you can effectively support and guide your organisation in navigating the process of implementing DORA within your specific area of responsibility.

Remember that digital resilience is a collaborative effort that requires commitment and collaboration across the entire organisation.

8. DORA dictionary: Key concepts and terms

To navigate the complexities of DORA and related regulations, here is a dictionary of some of the most commonly used technical terms:

DORA (Digital Operational Resilience Act): An EU regulation designed to strengthen digital resilience among financial institutions. It covers a wide range of requirements from IT security to managing third-party risks.

RTS (Regulatory Technical Standards): Detailed rules developed by the European Supervisory Authorities to ensure uniform application of the legislation. The RTS specifies how financial institutions must meet certain parts of the requirements of DORA.

ITS (Implementing Technical Standards): Similar to the RTS but focuses more on the technical aspects of implementing legislation. The ITS provides guidance on how to implement the technical elements of the regulation in practice.

Risk management: The process of identifying, assessing and controlling threats to an organisation's capital and earnings. In the context of DORA, the focus is specifically on risks associated with IT systems and digital processes.

Third-party risk: The risk associated with outsourcing operational functions to external providers, such as cloud services or IT support. DORA requires financial institutions to have processes in place to identify, assess and manage these risks.

Operational resilience: The ability to effectively prepare for, respond to and recover from operational disruptions to continue critical operations. This includes cyberattacks and other threats to daily operations.

Cyber resilience: A subset of operational resilience that specifically focuses on withstanding, responding to and recovering from cyberattacks.

Incident reporting: The requirement to report significant IT security incidents to relevant authorities. This gives authorities insight into the current threat landscape and helps strengthen the overall resilience of the sector.

Digital infrastructure: The overall structure of IT systems and networks that an organisation uses to conduct its business. DORA requires financial institutions to take measures to protect their digital infrastructure from threats.

Contact

For more information, please contact:

Louise Mehl
Implement Consulting Group
+45 5221 6316
lome@implement.dk

Claus Andersen
Implement Consulting Group
+45 4042 3770
cand@implement.dk

Pernilla Nordström
Implement Consulting Group
+46 729 809 063
pern@implement.se

Thomas Hedegaard
Implement Consulting Group
+45 2090 9670
thed@thetechcollective.eu

Christopher Juel Bendtsen
Implement Consulting Group
+45 2730 9700
chbe@implement.dk