SECURVANCE

Step-by-step Guide -

DORA (Digital Operational Resilience Act).

Introduction

The Digital Operational Resilience Act (DORA) is a regulation by the European Union, designed to enhance the operational resilience of financial institutions in an increasingly digital world. DORA sets strict requirements on how organizations manage their digital resilience, ensuring they are better equipped to withstand cyberattacks and other digital threats. Compliance with DORA is not only a legal obligation but also a strategic necessity for financial institutions to ensure the continuity and security of their services.

This guide provides a step-by-step approach for implementing DORA within your organization. We begin with the statement of applicability, outlining the specific requirements relevant to your organization. Next, we perform a gap analysis to identify areas where your current practices fall short of DORA standards. Following this, we develop a gap closure plan to address these deficiencies. For medium and low priority gaps, we conduct a thorough risk analysis to determine appropriate mitigation strategies. Finally, we move to the implementation phase, where we put the necessary measures into practice. By following these steps, you can ensure that your organization not only meets DORA requirements but also becomes stronger and more resilient in the digital age.

Digital Operational Resilience Act

The primary objective of DORA is to ensure that financial entities, including banks, insurers, investment firms, and other financial service providers, implement measures to improve their digital resilience. This includes the ability to effectively respond to and recover from ICT-related incidents to maintain the continuity of critical services. DORA sets out specific requirements for risk management, incident reporting, testing procedures, and third-party providers of ICT services.

The core components of DORA include:

- **ICT Risk Management**:

Financial entities must implement comprehensive risk management systems that cover the identification, assessment, and mitigation of ICT risks. This involves having a detailed overview of their ICT assets and the associated risks.

- **Incident Reporting**:

DORA requires financial entities to have standardized procedures for reporting significant ICT incidents to the relevant authorities. This not only aids in a swift response to incidents but also promotes transparency and collaboration among various stakeholders.

- **Testing Digital Resilience**:

Entities must regularly test their ICT systems to identify vulnerabilities and weaknesses. This includes penetration testing and other forms of cybersecurity exercises.

- **Third-Party Management**:

As many financial entities rely on external service providers for their ICT needs, DORA imposes requirements on managing these relationships. Entities must ensure robust contractual agreements and regularly monitor the performance and security of their external partners.

- **Operational Continuity**:

Financial entities must have plans and procedures in place to ensure the continuity of their services, even in the event of severe ICT disruptions. This includes disaster recovery plans and periodic exercises to test the effectiveness of these plans.

By complying with DORA's requirements, financial entities can not only better manage the risks associated with digital disruptions but also enhance the trust of their customers. DORA fosters a culture of proactive risk management and continuous improvement, making the sector more prepared for the challenges of digital transformation.

Phase 1. Statement of Applicability

Identify which specific aspects of DORA apply to the organization

The Statement of Applicability (STAP) is a foundational step in DORA compliance, where the organization determines which specific provisions and requirements of the DORA apply to its operations.

During phase 1, Securance Advisory will prepare a STAP-document for all main themes based on organizational characteristics and corresponding proportionality. This document will establish the extent to which the DORA legislation applies and to which components.

The STAP will be reported and discussed with stakeholders. After approval by the client, the STAP report will serve as the starting point for the next phase.

Actions

- **Analyse the business activities and technologies**
  Securance Advisory conducts a comprehensive review of the organization's operations, technology stack, and service offerings to understand the scope of applicability.

- **Identify relevant DORA provisions**
  Securance Advisory created a comprehensive document that outlines all the DORA requirements. Within the STAP, an analysis will be performed to make sure only the provisions are used that apply to the organization. This document includes detailed justifications for why each requirement is applicable or not applicable with, where needed, references to other legal provisions.

By completing the STAP, the organization establishes a clear and tailored framework for its DORA compliance efforts. This step ensures that subsequent actions are focused on the specific regulatory requirements that are relevant to the organization.

Phase 2. Fit-Gap analysis level 1 and level 2

Assess the current state of the organization against DORA's requirements

Assess the current state of the organization against the requirements of the DORA to identify areas of compliance (FIT) and non-compliance (GAP).

By conducting a thorough FIT-Gap Analysis, the organization can clearly understand where it stands in relation to DORA compliance, which areas are already covered, and which gaps need to be addressed. This analysis forms the basis for the subsequent steps in the compliance project, ensuring a focused and efficient approach to achieving full compliance with DORA.

Securance Advisory compiled a list of DORA requirements to align the organization's existing practices with these standards, identifying points of convergence and areas of deviation.

Actions:

- **Identify FIT areas**
  Clearly document the areas where the organization already meets DORA requirements. This could include existing policies, procedures, and technical controls that align with DORA's standards.

- **Highlight non-compliance areas**
  Identify and document the areas where the organization does not meet DORA requirements. This could involve missing policies, inadequate controls, or outdated procedures.

- **Assess priority of gaps**
  Evaluate the priority of each identified gap based on the potential impact on the organization and the likelihood of exploitation. Consider the criticality of the affected systems and processes.

- **Engage with stakeholders**
  Where needed, hold interviews with relevant stakeholders across different departments to gather detailed insights into current practices and to validate the identified gaps.

- **Review and validate**
  Conduct an internal review of the FIT-Gap analysis report with the project team and senior management to ensure its accuracy and comprehensiveness.

- **Create a FIT-Gap analysis report**
  Develop a detailed report that outlines the findings of the FIT-Gap analysis. This report includes:
  1. A comprehensive list of DORA requirements
  2. Summary and synthesis
  3. Identified gaps
  4. Prioritization of gaps
  5. Introduction to Gap Closure Plan

Phase 3. Gap Closure Plan

Develop a comprehensive plan to address the identified gaps and achieve compliance with the DORA

This step involves outlining specific actions for the high priority gaps and allocating resources to ensure that all compliance requirements are met effectively.

The Gap Closure Plan includes the following:

- **Analysis of both the current and desired situation**
  For each GAP, both the current situation and the desired situation are described. This will form the basis for the actions that will be defined. The desired situation includes clear, measurable objectives that align with DORA requirements and address the identified gaps.

- **Define specific actions and measures**
  Identify actions for each identified GAP, specifying what needs to be done, who will be responsible, and what resources will be required.

- **Set priorities and timeline**
  Develop a realistic timeline for each action, considering the complexity of the tasks and the availability of resources.

- **Implementation preparation**
  Create detailed implementation plans that outline the steps needed to execute each remediation action. This includes preparing any necessary documentation, training materials, and communication plans.

- **Document and report:**
  Provide a report that summarizes all of the above and potential first steps to implement the actions mentioned in the Gap Closure Plan. These reports will be presented and are open to feedback.

By following these steps, the organization can ensure a systematic and effective approach to closing identified gaps and achieving compliance with DORA.

Phase 4. Risk Analysis for medium and low priority GAPs

Assess the risks associated with the identified gaps and prioritize actions

Prioritize the identified low and medium priority gaps based on their potential impact on the organization's digital operational resilience and the complexity of closing each GAP.

Actions

- **Conduct risk analysis**
  Assess the severity of each risk by considering both its potential impact on the organization and the likelihood of its occurrence. Use qualitative and quantitative methods to evaluate these risks.

- **Assess impact and likelihood:**
  Determine the potential consequences of each risk on the organization. Evaluate the probability of each risk occurring. Factors influencing likelihood may include the organization's current controls, historical incidents, industry trends, and vulnerability to specific threats.

- **Create a risk matrix**
  Develop a risk matrix that plots the likelihood of each risk against its potential impact. This visual tool helps categorize risks into different levels of severity. Based on the matrix, categorize each risk into appropriate levels.

- **Develop priority list**
  Develop a prioritized list of risks based on their severity levels from the risk matrix. Focus on addressing the most critical risks first to mitigate the highest potential impacts on the organization.

- **Action planning**
  For each prioritized risk, outline specific actions and measures needed to mitigate the risk. This might include enhancing security controls, updating policies, implementing new technologies, or conducting additional training.

- **Develop timeline**
  E.stablish realistic timelines for implementing the risk mitigation actions. Prioritize actions that address critical risks with the highest impact and likelihood.

- **Documentation and reporting**
  Keep detailed records of all risk assessments, including the rationale for impact and likelihood ratings and the prioritization decisions.

By following these steps, the organization can effectively assess and prioritize the risks associated with the identified gaps, ensuring that resources are focused on the most critical areas.

Phase 5. Implementation

Implementing the actions

This step ensures that resources are allocated efficiently, focusing on the most critical areas to mitigate significant risks first.

Actions

- **Execution of the Gap Closure Plan**
  This involves implementing specific actions to address the gaps identified during the FIT-Gap Analysis. These actions could include updating policies and procedures, enhancing technology infrastructure, implementing new security measures, or improving operational processes. Our team can assist you by providing tailored recommendations and hands-on support to ensure these actions are carried out effectively.

- **Communicating policy and process changes**
  It's crucial to communicate any changes in policies, procedures, or practices to relevant stakeholders within the organization. This ensures that everyone understands their roles and responsibilities in compliance with DORA requirements.

- **Testing and validation**
  Implementing DORA compliance measures involves testing systems and processes to ensure they work as intended. Our consultants can guide you through rigorous testing and validation procedures, ensuring that your systems meet all necessary standards and operate seamlessly.

- **Monitoring and reporting**
  Establishing mechanisms to monitor ongoing compliance with DORA requirements. This could involve setting up regular audits, assessments, or continuous monitoring systems to detect and address any deviations or issues promptly.

- **Documentation and reporting**
  Maintaining comprehensive documentation of all implemented measures, changes, and compliance activities. This documentation is essential for demonstrating compliance during regulatory audits or inquiries. We provide templates and best practices for documentation, ensuring that your records are thorough and audit-ready.

- **Review and continuous improvement**
  Periodically reviewing the implemented measures to assess their effectiveness and identify areas for improvement. Continuous improvement ensures that the organization remains resilient to digital operational risks over time. Our team can conduct regular reviews and suggest improvements, helping you stay ahead of potential risks.

- **Adaptation to evolving requirements**
  Given the dynamic nature of regulatory requirements, staying updated with any changes or updates to DORA and adapting the implementation plan accordingly. We keep track of regulatory changes and can help you adapt your compliance strategy as needed, ensuring you are always up-to-date with the latest requirements.

By following a structured approach to implementation, organizations can enhance their digital operational resilience and ensure compliance with DORA requirements effectively.

Contact

Looking to promptly comply with the DORA?

Our handy quick guide offers a straightforward, step-by-step approach to achieving compliance. Our expert team is ready to guide you through the five phases of this approach, from conducting an initial assessment to implementing operational improvements. All of this is done while incorporating our best practices and using our templates. Let us assist you in strengthening your digital operational resilience and preparing your business for the future.

Contact us today at the number below for further clarification, consultation, and/or a quote for support, ensuring you're well-supported and confident in achieving timely DORA compliance.

Securance

63-66 Hatton Garden

London EC1N 8LE, UK

+44 20 351 446 56

www.securance.co.uk

Securance BV

Reactorweg 47

3542 AD Utrecht

+31 (0)30 2800888

www.securance.nl

Securance Sweden

Sidenvävargatan 17

753 19 Uppsala

+46703040656

Securance Germany

Josef-Orlopp-Straße 54

10365 Berlin

+4930439716860

BECOME THE ARCHITECT OF YOUR FUTURE

SECURANCE

Office The Netherlands
Address: Reactorweg 47 (4th floor)
3542 AD Utrecht, The Netherlands
Tel: +31(0)30 280 08 88
Mail: info@securance.com

Office United Kingdom
Address: 63-66 Hatton Garden
Londen EC1N 8LE, United Kingdom
Tel: +44 (0)20 351 446 56
Mail: info@securance.com