Deloitte.

DORA & Third-Party Risk Management

Assessing and showing compliance with DORA

A reference guide to DORA TPRM and Deloitte's attestation services

Deloitte.

Table of Contents

DORA and Third-Party Risk Management

The Digital Operational Resilience Act (DORA) is a proposed legislation in the European Union that aims to enhance the resilience of the financial sector by addressing the risks arising from digital operational incidents. One of the key areas that the DORA seeks to regulate is third-party vendor risk management.

What does compliance look like

The following are the main requirements for third-party vendor risk management under DORA:

- **Identification and assessment of critical third-party service providers:** Financial institutions must identify and assess the criticality of their third-party service providers based on their impact on the institution's operations and the level of risk they pose.

- **Due diligence and contractual requirements:** Financial institutions must conduct due diligence on their third-party service providers to ensure that they have appropriate risk management practices and contractual requirements in place to manage the risks.

- **Ongoing monitoring and oversight**: Financial institutions must continuously monitor and oversee their third-party service providers to ensure that they comply with contractual requirements, manage risks appropriately, and maintain their resilience.

- **Incident management and reporting:** Financial institutions must have processes in place to manage and report incidents related to their third-party service providers.

- **Contingency planning and testing:** Financial institutions must have contingency plans in place to address potential disruptions to their services caused by third-party service provider incidents. They must also conduct testing to ensure that these plans are effective.

Overall, the DORA requires financial institutions to take a risk-based and proactive approach to third-party vendor risk management to ensure that they maintain their operational resilience in the face of digital operational incidents.

The increasing reliance of financial institutions on third-party service providers to deliver their services has resulted in a complex web of relationships that can lead to significant operational risks. These risks can arise from factors such as data breaches, cyber-attacks, system failures, and inadequate risk management practices of third-party vendors. By mandating appropriate risk management practices for third-party vendors, DORA seeks to reduce the operational risks associated with these relationships and ensure the resilience of the financial sector.

DORA also seeks to establish a harmonized regulatory framework for third-party vendor risk management across the European Union. This framework will provide a level playing field for financial institutions and third-party vendors operating across the EU and ensure that they comply with common standards and best practices. This will help to enhance the overall resilience of the financial sector, reduce compliance costs for financial institutions, and improve the transparency and accountability of third-party vendors.

DORA also recognizes the need for financial institutions to have a proactive and risk-based approach to third-party vendor risk management. By requiring financial institutions to identify and assess the criticality of their third-party vendors, conduct due diligence, and continuously monitor and oversee them, DORA ensures that financial institutions are better prepared to manage the risks associated with third-party relationships. This will help to prevent incidents before they occur, mitigate the impact of incidents that do occur, and improve the overall resilience of the financial sector.

Are you in scope of DORA?

To determine if you are in the scope of the DORA regulation, you should consider the following:

- **Type of entity:** DORA applies to all financial entities, including credit institutions, investment firms, payment institutions, electronic money institutions, and insurance and reinsurance undertakings.
- **Geographic location:** DORA applies to all financial entities that operate in the EU, regardless of where they are based.
- **Size and complexity:** DORA applies to financial entities of all sizes and complexities, but the requirements and expectations may vary depending on the entity's size and complexity.
- **Activities:** DORA applies to all activities that are critical to the provision of financial services, including IT systems and services, cybersecurity, data management, outsourcing, and business continuity management.

If you fall within the scope of the DORA regulation, you will need to comply with its requirements, which include conducting regular risk assessments, establishing and maintaining robust IT and cybersecurity systems, and having effective business continuity plans in place. You may also be subject to regular supervisory reviews and audits to ensure compliance with the regulation.

All areas in scope of DORA

The areas in scope for the DORA regulation include:

- **Business continuity management:** This covers the financial institution's ability to continue operations in the event of a disruption, including disaster recovery and incident response plans.
- **Information security:** This includes measures taken to protect data, systems, and networks from unauthorized access, as well as processes for identifying, assessing, and responding to security risks.
- **Data integrity and resilience:** This covers the accuracy, completeness, and consistency of data used by the financial institution, as well as processes for backup, recovery, and archiving.
- **Third-party risk management:** This includes processes for managing risks associated with third-party service providers, such as cloud providers or software vendors.
- **Incident reporting and management:** This covers the financial institution's processes for reporting and managing incidents that could impact its operations, including both internal and external incidents.
- **Governance and oversight:** This includes the financial institution's overall governance framework, as well as oversight of its technology operations and risk management practices.

What does it take to develop a DORA Attestation?

All of our attestation engagements follow the same general process. We have found that it is important to spend enough time up-front to get the scoping of the report right, develop a detailed plan of action, identify key stakeholders and make the practical arrangements. We have developed templates and, although each client's control environment is different, we have a good understanding of what types of controls to look for.

Planning, walkthroughs and gap analysis reporting

Phases 1 and 2 of any new DORA project includes planning the engagement, getting to know the key stakeholders and getting them used to the audit process and performing the initial process walkthroughs to identify control gaps or weaknesses. If we can get this analysis done early, the client is able to initiate remediation efforts to fill the control gaps and strengthen any weak controls early enough so that the rest of the testing process is as smooth as possible, and the resulting report is as free for 'findings' as possible.

Type 1 reporting

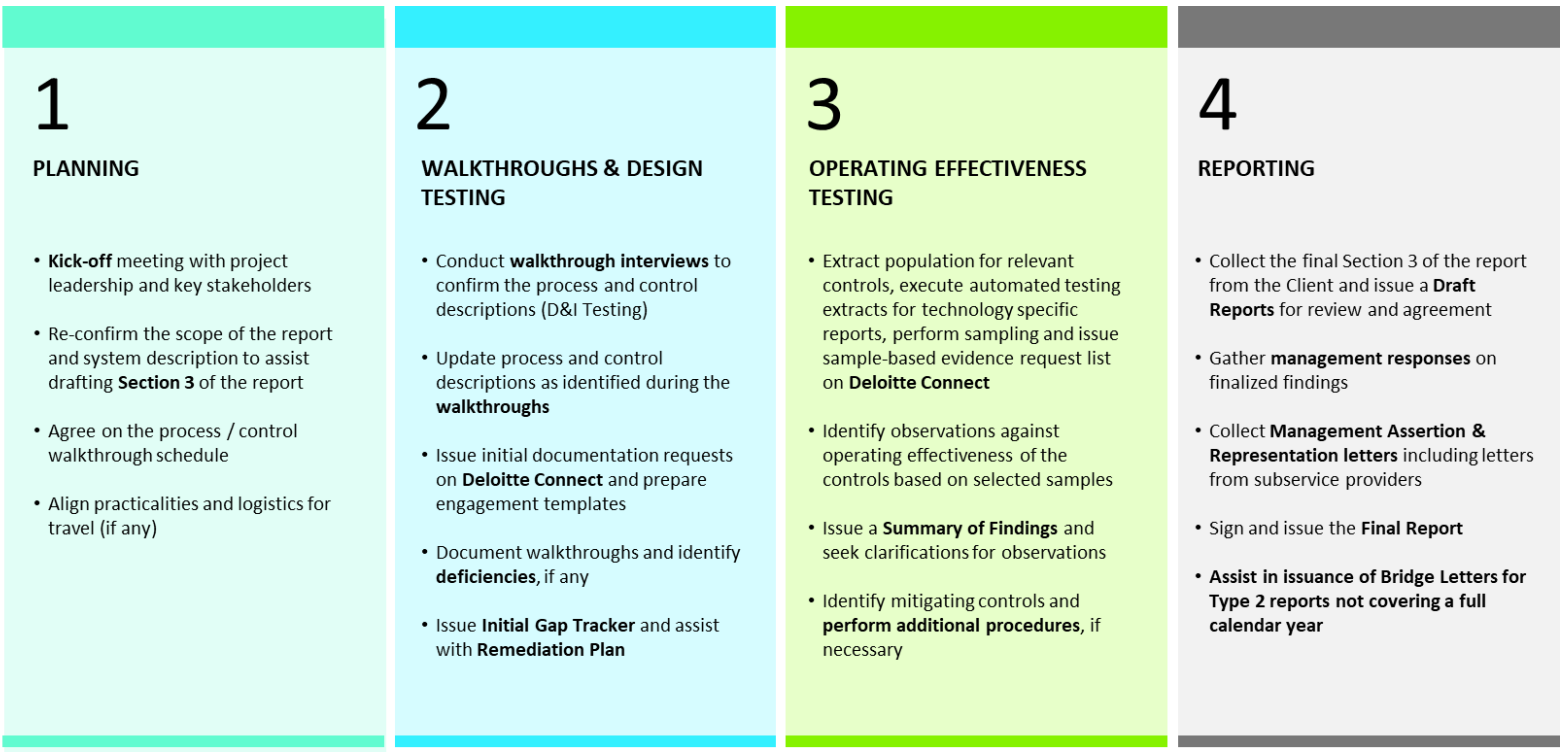
When the client is confident that any significant control gaps or weaknesses have been remediated, we perform the final control walkthroughs and assessment of the design and implementation of the controls necessary to produce the Type 1 version of the report. Most clients begin their attestation process by issuing a Type 1 report, saving the Type 2 reports for the future periods starting with the as-of date of the Type 1.

Type 2 reporting

When issuing a Type 2 report, we perform tests of the controls covering a period of time (at least 6 months), general from 01. January through to 31.December. These detailed tests are performed using internationally accepted audit sampling guidelines, which are designed to provide reasonable assurance that errors would be identified in the sample, if relevant.

Ongoing improvement

Discussing lessons learned with the client, tracking areas for future improvement with the report or our audit methods and regularly assessing the quality of our work ensures that our engagements and reports are of the highest quality.



Our Third-Party Related Services

We provide many types of attestations and other third-party related services. Our attestation subject matter experts work closely with Deloitte's other SME's with knowledge in specific fields to provide attestation reports covering a wide range of topics.

- **ISAE3402 / SOC 1 Attestation -** We deliver numerous ISAE3402 reports for customers each year and even have clients where we issue a combined ISAE3402 and SOC1 report, increasing the useability of the report for their US customer base. These reports are mostly used to evidence controls in place to ensure the completeness and accuracy in the processing of financial information.

- **SOC2 Attestation -** Performed in accordance with AICPA issued Trust Service Criteria for Confidentiality, Availability, Security, Processing Integrity and Privacy, we issue more than 10 SOC 2 reports for Norwegian companies annually.

- **Sustainability Attestation -** We provide attestation reports on companies' sustainability reporting as well as other Climate and Sustainability related topics.

- **GDPR (Data Processing Agreement) Attestation -** We provide attestations to customers which are used to evidence compliance with the terms outlined in their Data Processing Agreements.

- **DORA Attestation -** Based on the DORA Directive, we create a report of the controls you have in place to address each requirement, perform tests of each control and provide a summary of the results.

- **NIS 2 Attestation -** Based on the NIS 2 Regulation, we create a report of the controls you have in place to address each requirement, perform tests of each control and provide a summary of the results.

- **MITid Compliance Attestation -** For companies who are obligated to be in compliance with the Danish MitId requirements, we create a report of the controls you have in place to address each requirement, perform tests of each control and provide a summary of the results.

- **NSIS Compliance Attestation -** For companies who wish to show their adherence to the National Standard for Identity Assurance Levels (NSIS) framework, we create a report of the controls you have in place to address each requirement, perform tests of each control and provide a summary of the results.

- **Customer Specific Reporting -** Occasionally, a vendor's customer may require adherence to a specific set of requirements (e.g., a subset of one of the ISO standards or other criteria). We develop attestation reports covering the specific requirements of the customer and provide a report of the controls addressing each requirement and the results of our testing of each to evidence the vendor's compliance to the requirements.

- **Third Party Risk Management (TPRM) -** We help companies build their programs to evaluate their risk levels related to their third-party service providers and give each vendor a risk rating based on a variety of criteria, develop risk-area specific contract terms that allow for proper measurement and follow-up of obligations, develop diagnostic theme-based self-assessment questionnaires, develop programs for the periodic evaluation and follow-up with high-risk vendors, develop training program for those responsible for participating in the TPRM program and other aspects of TPRM (e.g., performing vendor audits, reviewing SOC reports and other evidence submitted by vendors as part of their response to a questionnaire)

- **Vendor Audits (Internal audit support or other)** – Often performed on behalf of a company's internal audit function or in response to a specific incident or identified risk at a vendor, we use our extensive knowledge of the various requirements, standards and criteria to develop situation specific audit programs to be executed at one or more vendors. We have standard report formats we can deliver to summarize the results of our audits or we use the company's specific reporting format.

Note: *The names of our references are made anonymous for this brochure.*

Engagement references

Our core team of Third-Party Assurance experts each has significant experience in providing attestation services.

Our client experience

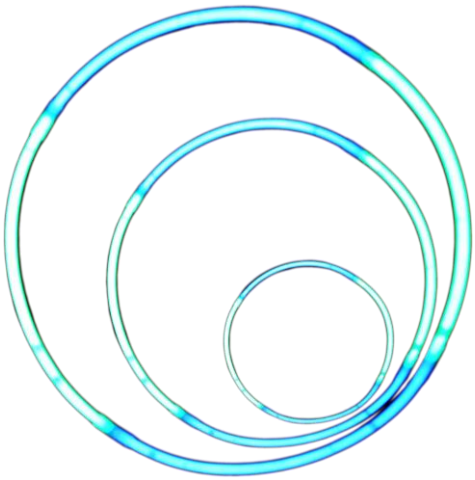
Our team of more than 90+ TPA resources in the Nordic region, supported by subject matter experts from our IT audit, Cyber Security, Financial Audit, Legal and Consulting departments, deliver more than 200 attestation reports to more than 100 clients in the region. We work on some of Nordic's most challenging and exciting attestation engagements.

The following is a list of some of the engagements our Norwegian Team has worked on or are currently delivering. We support engagements across the Nordic region, as indicated (NO, SE, DK).

- **Payroll processing** (ISAE3402 Type 2 - Payroll)
- **SaaS provider** (DORA Type 2 – SaaS))
- **SaaS provider** (ISAE3000 GDPR – SaaS) (DK)
- **Telecom** (ISAE3402 – Transaction processing)
- **SaaS provider** (ISAE3000 Type 1 – SaaS) (DK)
- **SaaS provider** (ISAE3000 GDPR – SaaS) (DK)
- **IT services provider** (DORA Type 2 – IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS) (DK)
- **Transportation services** (ISAE3402 Type 2 – Ticket income distribution)
- **IT services** (DORA Type 2 – IT) (DK)
- **Financial services** (ISAE3402 Type 2 – IT) (DK)
- **Educational Institution** (ISAE3402 Type 2 and ISAE3000 GDPR (DK)
- **SaaS provider** (DORA Type 2 - SaaS)
- **Financial services** (ISAE3402 and multiple DORA reports – Financial services) (SE)
- **IT services provider** (ISAE3402 Type 2 – Managed IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS)
- **IT security services** (DORA Type 2 – IT Services)
- **Airline** (ISAE3000 Type 1 – Process integrity)
- **SaaS provider** (DORA Type 2 – SaaS)
- **SaaS provider** (DORA Type 2 – SaaS)
- **IT services** (DORA Type 2, ISAE3402 Type 2 and ISAE3000 GDPR – Managed IT))
- **Financial services** (DORA+ with CSA CCM – Financial services) (DK)
- **SaaS provider** (ISAE3402 Type 1 – SaaS) (DK)
- **SaaS provider** (DORA Type 2, ISAE3000 GDPR and ISAE3000 for MitID and NSIS - SaaS)
- **IT services provider** (ISAE3402 / SOC1 combined and DORA Type 2 – Data center services)
- **SaaS provider** (ISAE3402 Type 2 and 3 ISAE3000 GCPR – SaaS) (DK)
- **IT services** (Multiple ISAE3000 reports – Managed IT Services)
- **SaaS provider** (ISAE3402 Type 2 – Visma Cloud Delivery Model)

Our customers will vouch for us

Considering using our services but uncertain? We can provide you with multiple client references that you can feel free to contact to discuss our team, our services and our quality. These references can be provided as part of a request for proposal discussion.



Contact information

Kevin F. McCloskey
Associate Partner, Third-Party Assurance Services
CISA, CIA, CIPP/e, CRMA
Mobile: +47 913 68 848
Email: kmccloskey@deloitte.no

Lasse Vangstein
Partner, State Authorized Auditor
Mobile: +47 975 84 086
Email: lvangstein@deloitte.no

Jouni Viljanen
Partner, Risk Advisory
Mobile: +35 820 755 5312
Email: Jouni.Viljanen@deloitte.fi