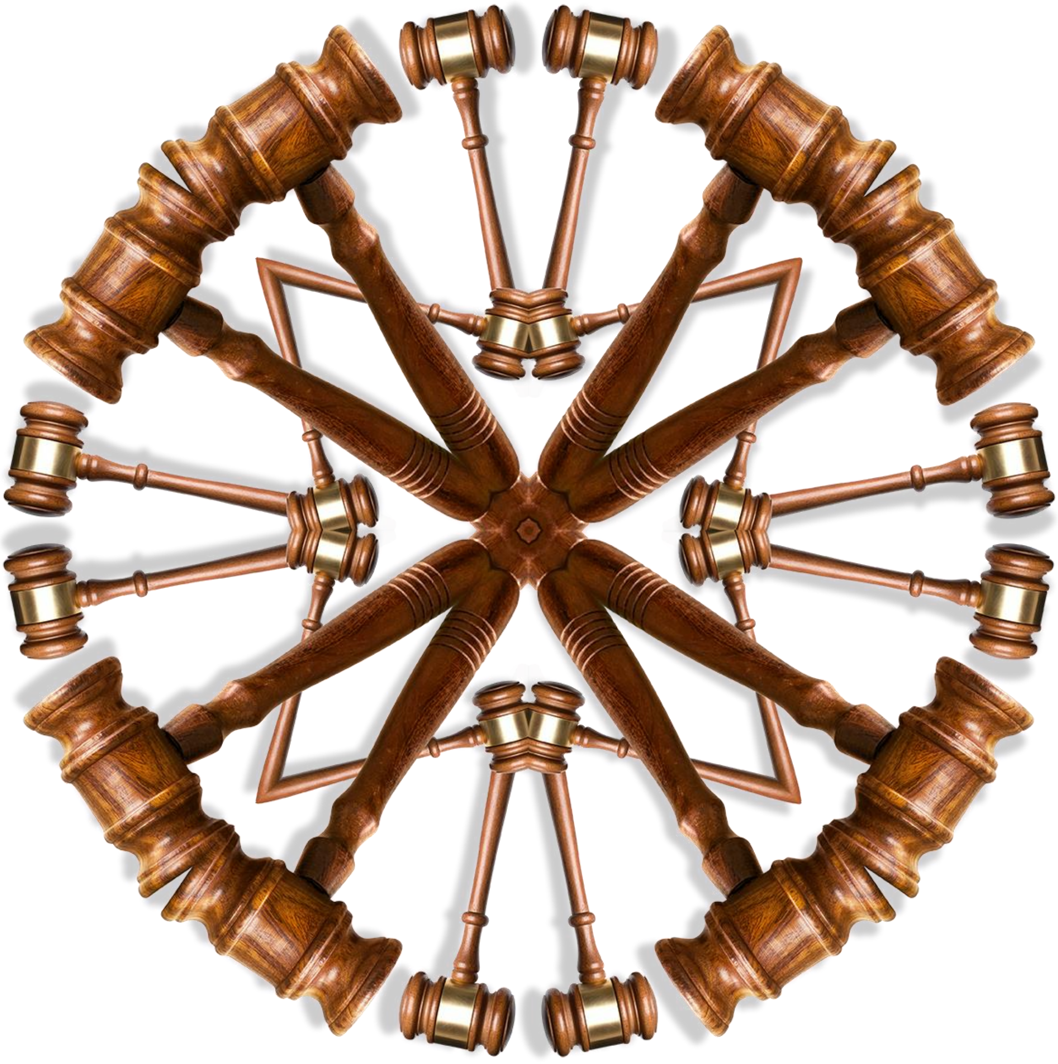
Deloitte.



NIS 2 Attestation

Compliance with the directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

A reference guide to NIS 2 and Deloitte's services

Table of Contents

NIS 2 Overview

Deloitte's Services

NIS 2 in a nutshell

The NIS2 Directive is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

The EU cybersecurity rules introduced in 2016 were updated by the NIS2 Directive that came into force in 2023. It modernized the existing legal framework to keep up with increased digitization and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

What does the Directive say?

The Directive on measures for a high common level of cybersecurity across the Union (the NIS2 Directive) provides legal measures to boost the overall level of cybersecurity in the EU by ensuring:

- Member States' preparedness, by requiring them to be appropriately equipped. For example, with a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority
- Cooperation among all the Member States, by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.
- A culture of security across sectors that are vital for our economy and society and that rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

The Directive requires member states to establish a competent authority responsible for overseeing the implementation of the directive and ensuring compliance by OES and DSPs. These authorities can impose fines and penalties on service providers that fail to comply with the regulations.

Businesses identified by the Member States as operators of essential services in the above sectors will have to take appropriate security measures and notify relevant national authorities of serious incidents. Key digital service providers, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements under the Directive. The NIS2 Directive requires operators of essential services (OES) in specific sectors, such as energy, finance, healthcare, and transport, to identify and manage their cybersecurity risks effectively. Additionally, it mandates digital service providers (DSPs) to follow security measures in a risk-based and proportional manner to ensure the security of their customers' data.

The directive can have a significant impact on service providers because they will need to take additional measures to ensure the security of their networks and systems. They must also establish incident response plans to react to cybersecurity incidents promptly. The directive's requirements will apply not only to businesses established within the EU but also to companies based outside the EU if they provide essential services or digital services within the EU.

Overall, the NIS2 Directive aims to increase the security of network and information systems and protect critical infrastructure and essential services from cyber threats. It may require service providers to increase their investment in cybersecurity and develop new policies and procedures to comply with the regulations.

Are you in scope of NIS 2?

The NIS 2 (Network and Information Systems) Directive is an EU-wide legislation that seeks to enhance the cybersecurity and resilience of network and information systems across critical sectors, such as energy, transport, healthcare, and finance. The directive's scope is defined in Annex I and Annex II and covers two main categories of entities.

Annex I

Annex I identifies Operators of Essential Services (OES) that are public or private entities providing essential services in critical sectors. The entities identified as OES may vary among member states but must meet the essential service criteria defined in Annex II. Examples of OES include electricity providers, transportation companies, and healthcare providers.

Annex I	Sub-sectors
Energy	Electricity, District heating and cooling, Oil, Gas
Transport	Air, Rail, Water, Road
Health	Pharma, Manufacturing, Laboratories, Services
Water	Drink and waste
Space	Infrastructure, Services
ICT	MSP, MSSP

Annex II

Annex II defines the criteria for identifying Digital Service Providers (DSPs) subject to the NIS 2 Directive. DSPs are entities that provide online services, such as search engines, cloud computing services, and online marketplaces. The DSPs that are subject to the directive are those that exceed certain thresholds in terms of number of users, turnover, and market share.

Annex II	Sub-sectors
Waste Mgmt	All
Food	Production, Processing, Distribution
Manufacturing	Chemicals, Medical Dev., Computer electronics, Optical products, Electrical equipment, Machinery & Equipment, Motor Vehicles, Trailers, Transport equipment
Postal / Courier	All

Obligations

Both OES and DSPs falling under the scope of the NIS 2 Directive are subject to various obligations, including taking appropriate security measures to manage risks and prevent incidents, reporting significant incidents to the relevant national authority, and undertaking regular security audits and assessments. Compliance with the NIS 2 Directive is mandatory for all entities falling under its scope, and non-compliance may result in significant fines and reputational damage.

In summary, the NIS 2 Directive's scope is determined by Annex I and Annex II, which identify the categories of entities subject to the directive's obligations. Compliance with the directive's requirements is essential for enhancing cybersecurity and resilience in critical sectors and protecting against cyber threats.

What does it take to develop a NIS 2 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 NIS 2 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

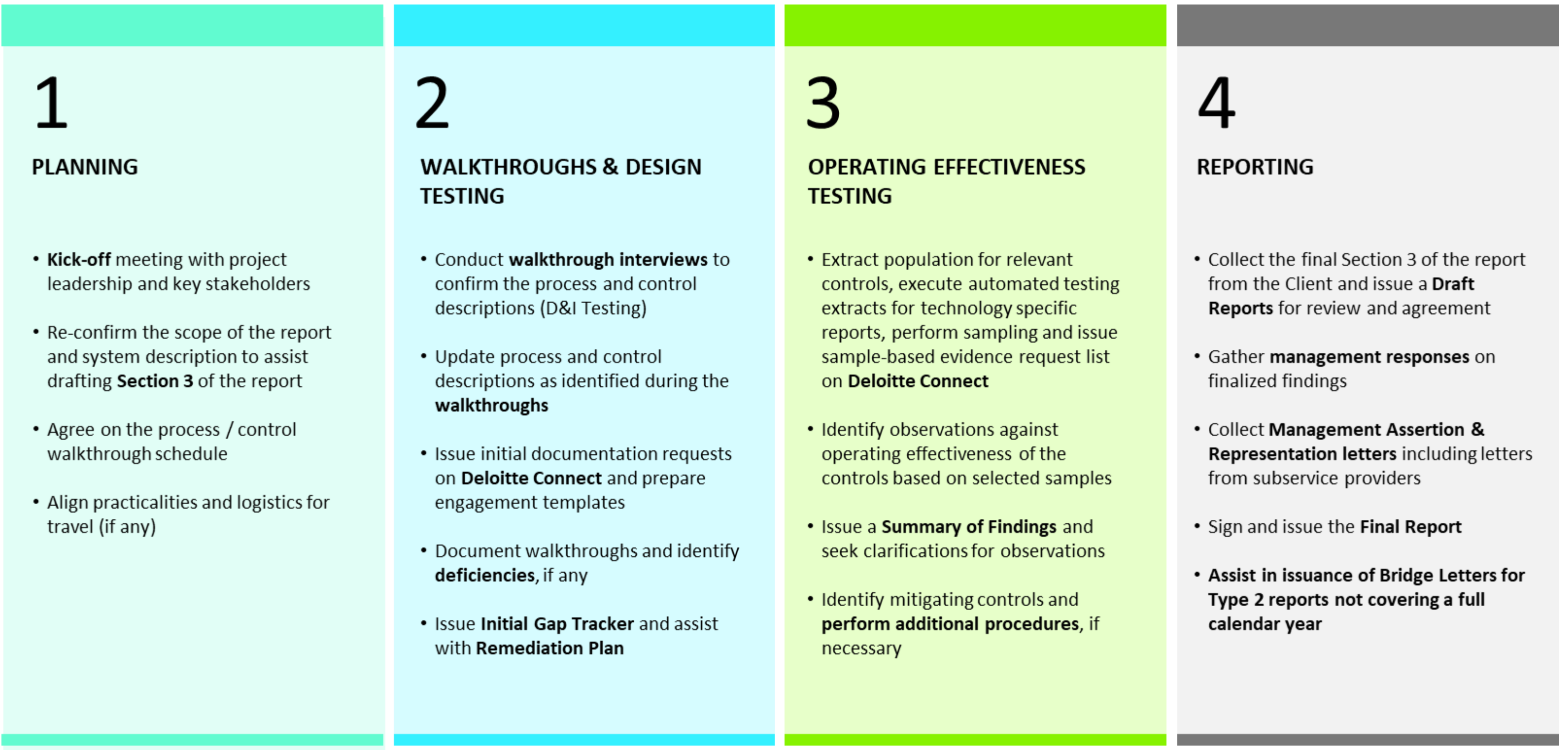
When the client is confident that any significant control gaps or weaknesses have been remediated, we perform the final control walkthroughs and assessment of the design and implementation of the controls necessary to produce the Type 1 version of the report. Most clients begin their attestation process 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.



1

PLANNING

- **Kick-off** meeting with project leadership and key stakeholders
- Re-confirm the scope of the report and system description to assist drafting **Section 3** of the report
- Agree on the process / control walkthrough schedule
- Align practicalities and logistics for travel (if any)

2

WALKTHROUGHS & DESIGN TESTING

- Conduct **walkthrough interviews** to confirm the process and control descriptions (D&I Testing)
- Update process and control descriptions as identified during the **walkthroughs**
- Issue initial documentation requests on **Deloitte Connect** and prepare engagement templates
- Document walkthroughs and identify **deficiencies**, if any
- Issue **Initial Gap Tracker** and assist with **Remediation Plan**

3

OPERATING EFFECTIVENESS TESTING

- Extract population for relevant controls, execute automated testing extracts for technology specific reports, perform sampling and issue sample-based evidence request list on **Deloitte Connect**
- Identify observations against operating effectiveness of the controls based on selected samples
- Issue a **Summary of Findings** and seek clarifications for observations
- Identify mitigating controls and **perform additional procedures**, if necessary

4

REPORTING

- Collect the final Section 3 of the report from the Client and issue a **Draft Reports** for review and agreement
- Gather **management responses** on finalized findings
- Collect **Management Assertion & Representation letters** including letters from subservice providers
- Sign and issue the **Final Report**
- **Assist in issuance of Bridge Letters for Type 2 reports not covering a full calendar year**

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.

- **NIS 2 Attestation -** Based on the NIS 2 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.

- **DORA Attestation -** Based on the DORA 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** (NIS 2 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** (NIS 2 Type 2 – IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS) (DK)
- **Transportation services** (ISAE3402 Type 2 – Ticket income distribution)
- **IT services** (NIS 2 Type 2 – IT) (DK)
- **Financial services** (ISAE3402 Type 2 – IT) (DK)
- **Educational Institution** (ISAE3402 Type 2 and ISAE3000 GDPR (DK)
- **SaaS provider** (NIS 2 Type 2 - SaaS)
- **Financial services** (ISAE3402 and multiple NIS 2 reports – Financial services) (SE)
- **IT services provider** (ISAE3402 Type 2 – Managed IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS)
- **IT security services** (NIS 2 Type 2 – IT Services)
- **Airline** (ISAE3000 Type 1 – Process integrity)
- **SaaS provider** (NIS 2 Type 2 – SaaS)
- **SaaS provider** (NIS 2 Type 2 – SaaS)
- **IT services** (NIS 2 Type 2, ISAE3402 Type 2 and ISAE3000 GDPR – Managed IT))
- **Financial services** (NIS 2+ with CSA CCM – Financial services) (DK)
- **SaaS provider** (ISAE3402 Type 1 – SaaS) (DK)
- **SaaS provider** (NIS 2 Type 2, ISAE3000 GDPR and ISAE3000 for MitID and NSIS - SaaS)
- **IT services provider** (ISAE3402 / SOC1 combined and NIS 2 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

Kevin is responsible for Deloitte Third Party Assurance (TPA) services in Norway and has over 30 years of experience working with TPA Services, IT audit, Internal Audit and IT-based internal control in general. He has recent experience from, among other projects, the delivery of numerous ISAE3402 / SOC1, SOC2 and ISAE3000 attestations, several large Third-Party Risk Management projects and several internal audit assistance engagements.

Kevin has written several articles focused on Third Party Risk Management, Third Party Assurance and Attestation and GDPR Assurance. He is a subject matter expert in Deloitte in regard to TPA and TPRM. Kevin presents these topics to both internal and external audiences and is a former lecturer in IT Auditing at NHH's Master program.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.no for a more detailed description of DTTL and its member firms.

Deloitte Norway conducts business through two legally separate and independent limited liability companies; Deloitte AS, providing audit, consulting, financial advisory and risk management services, and Deloitte Advokatfirma AS, providing tax and legal services.