Deloitte.

ISAE3402 Reporting

Assurance Reports on Controls at a Service Organization

A reference guide to ISAE3402 and Deloitte's services

Table of Contents

ISAE3402 Overview

Deloitte's ISAE3402 Services

ISAE3402 Overview

ISAE3402 in a nutshell

There is an increasing demand for Norwegian companies to provide independent assessments of their internal controls in place around the products and services they deliver to their customers. Customers (and their auditors) are requiring confirmation that there is a mature internal control environment in place that ensures the completeness and accuracy of the financial information being processed by the service organizations. A common way to meet this requirement is for the service provider to provide an annual ISAE3402 report to the customer(s). Some service organizations are also seeing the commercial advantage of being able to provide these reports as part of contract negotiations or in bids for new customers.

What is an ISAE3402 Report?

ISAE 3402 (International Standard on Assurance Engagements 3402) is a framework that outlines the requirements for reporting on controls at a service organization, such as a cloud provider, an IT infrastructure provider. The standard is intended to provide assurance to customers and other stakeholders that the service organization has appropriate controls in place to ensure the confidentiality, integrity, and availability of the service organization's information systems.

Who needs to issue an ISAE3402 Report?

Companies that provide services that could impact the financial reporting of their clients, such as third-party payroll, accounting service or other financial transaction processing providers, data centers, software as a service (SaaS) providers and managed IT services providers would normally be asked to issue an ISAE3402 report if their customers process a significant amount of transactions through their products or services.

Type 1 vs. Type 2 Reports

In a ***Type I report****, the auditor expresses an opinion on (1) whether the service organization's description of controls presents fairly, in all material respects, the relevant aspects of their controls that had been placed in operation* ***as of a specific date****, and (2) whether the controls were suitably designed to achieve specified control objectives, established by the service organization.*

In a ***Type II*** *report, the service auditor expresses an opinion on the same items noted above in a Type I report, and (3) whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during* ***a period of time*** *(often 01 January through 31 December of a given year).*

The life cycle of an ISAE3402 Report

Step 1: Get the contract right (and fair)

We have often been involved in advising service organizations during their contract negotiations with the company requesting the report. It is important to get the wording correct in the contract, set realistic expectations for delivery timelines and to ensure that the scope of the report is correct. Issues like covering the cost of the effort, the type of report required and the timeline for delivery are significant.

Step 2: Gap analysis and remediation

We recommend starting off any IISAE3402 engagement with a set of gap analysis workshops. We meet with key personnel at the service organization to walk through the requirements and identify potential gaps or weaknesses in controls that need to be remediated.

Step 3: Type 1 reporting

Setting the ambition level to issue a Type 1 report first is recommended. This allows the service organization to get the control structure in place and to identify and remediate significant gaps or weaknesses while providing the recipient with a good 'first step in the right direction'. This will be the 'baseline' for which all future Type 2 reports can build and the controls in the Type 1 report would be executed and documented to ensure compliance with Type 2 testing requirements.

Step 4: Type 2 reporting

A Type 2 report tests the operational effectiveness of the controls over a period of time (e.g., 1 year) and requires good audit evidence of controls having been executed. The auditor will include a separate section in the report detailing the results of tests performed.

Step 5: Reevaluation and streamlining

The control regime, scope of the report and its contents and the methods and techniques used to test the controls should be reviewed at least annually to ensure ongoing relevance and efficiency.

Benefits of an ISAE3402 Report

Obtaining an ISAE3402 report requires investment both in terms of time and cost for an organization. However, the advantages of getting an ISAE3402 attestation are far more than the initial investment. Third party organizations that successfully complete an ISAE3402 audit can offer their clients reasonable assurance that an independent reviewer has assessed their controls that relate to ensuring that their product / services are processing their customers' financial information completely and accurately. The report helps to prioritize risks in order to ensure that high quality services are being delivered to the clients. Essentially, an ISAE3402 report is a tool that can give organizations a competitive advantage and open up their market to new geographies and industries.

Benefits for Service Organization

✓ **Commercial advantage:** In sales situations, ISAE3402 reports can be one of the items which differentiate one service organization from its peers/competitors. It may also be seen as a disadvantage if the provider does not have such a report, but their competitor does.

✓ **Cost savings:** Providing ISAE3402 reports, which require one audit team for a predictable period of time, is generally more cost effective than participating in customer audits. Customers receiving TPA reports are sometimes asked to pay for the reports, further reducing the cost burden of internal control testing.

✓ **Broad assurance:** Most ISAE3402 reports provide reasonable assurance to a broad range of clients with a single report.

✓ **Compliance requirements:** The ISAE3402 reports can demonstrate to regulatory bodies that controls are in place and operating effectively.

✓ **Improve overall control awareness:** The process of developing and issuing an ISAE3402 report at an service organization often generates increased internal control awareness within the organization.

✓ **Customer requirement:** Future customers / existing customers wishing to renew contracts may require ISAE3402 reports and having the report in place may lead to increased ability to win new customers or keep existing relationships.

Benefits to users of the ISAE3402 report

✓ **Confidence:** Increased confidence that the vendor is meeting the internal control expectations of their customers through independent and transparent reporting on operational effectiveness of controls at the service provider

✓ **Internal reporting requirements:** Ensuring that the company's multi-purpose reporting requirements — including operational and financial—are met

✓ **Valuable insight/monitoring:** Independent assessments of whether the controls of the service provider were in place, suitably designed and operating effectively, with a focus on continuous improvement when controls are found to be lacking

✓ **Cost savings:** Service providers may charge customers for the ISAE3402 reports, or they may not. The cost of being required to pay for an ISAE3402 report should be weighed against the cost of the customer having to maintain their own staff or hiring staff to be able to perform regular audits of the service providers.

✓ **Compliance requirements:** The ISAE3402 reporting process can contribute to the ongoing compliance with industry, governmental and other relevant regulatory requirements

What does it take to develop and issue an ISAE3402 Report?

Each of our ISAE3402 engagements has roughly followed the same 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 ISAE3402 project includes planning the engagement, getting to know the key stakeholders and getting them used to the ISAE3402 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

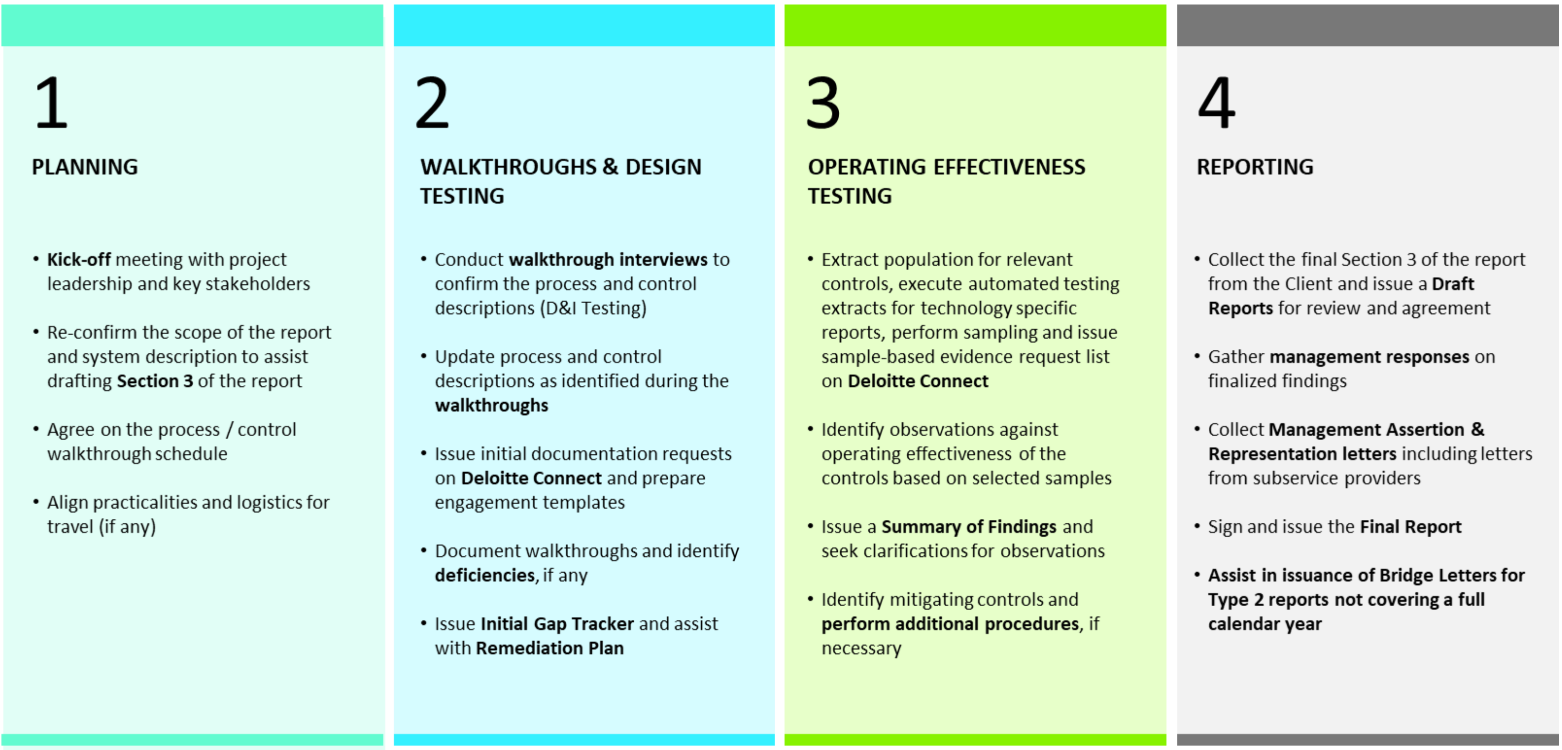
When the client is confident that any significant control gaps or weaknesses have been remediated, we perform the final control walkthroughs and assessment of the design and implementation of the controls necessary to produce the Type 1 version of the report. Most clients begin their reporting process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

Components of an ISAE3402 report

Report section	Description
Section I: Independent service auditor's report (opinion)	**Section I of an ISAE3402 report contains the service auditor's opinion about whether:** • Management's description of the service organization's system is fairly presented • The controls related to the control objectives stated in the description were suitably designed • For Type 2 reports only - The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period under review.
Section II: Management's Assertion provided by the Service Organization and Subservice Organization(s)	**Management is required to provide a written assertion about whether, in all material respects and based on suitable criteria:** • Management's description of the service organization's system fairly presents the service organization's system that was designed and implemented as of a specified date • The controls stated in management's description of the service organization's system operated effectively throughout the specified period to meet the control objectives • Management must have a reasonable basis for its assertion. Standards provide flexibility in the actual procedures performed by management. Management may not rely solely on the testing done by the service auditor.
Section III: Description of the system (provided by the service organization)	**Section III: System Description Overview (provided by the service organization)** • Overview • The types of services provided • The company's principal service commitments and system requirements • The components of the system to provide the services ○ Governance and organization ○ IT infrastructure and data flows ○ Business processes, control objectives and controls – see "*Common in-scope processes*" slide • Incidents occurring in the 12 months prior to report as of date that resulted in a significant impairment of Company XYZ's ability to achieve its service commitments and system requirements • Complementary user entity controls • Sub-service organizations
Section IV: Information Provided by the Service Auditor (Testing and Results)	• Overview of types of procedures performed to verify controls • A matrix of the control objectives and controls as defined in Section III • For each control, a description of the tests performed and the results of testing
Section V: Other information provided by the service organization (Optional)	**Other Information Provided by the Service Organization (Optional)** • Section V will contain information that the service organization would like to provide to the users of the report, which is NOT covered by the auditor's opinion.

Common in-scope processes

Accounting Services

- **Control environment, risk assessment and monitoring**
  - Corporate Governance
  - Risk Management and Internal control
  - Organizational Structure
  - Human Resources Policies and Practices (hiring, evaluations and continuous education)
- **Customer onboarding, maintenance and offboarding**
- **Personnel management**
- **Maintaining payroll master files**
- **Recording time**
- **Calculating payroll**
- **Disbursing payroll**
- **IT (Infrastructure, Applications, Security, Operations and Change)**

Payroll Services

- **Control environment, risk assessment and monitoring**
  - Corporate Governance
  - Risk Management and Internal control
  - Organizational Structure
  - Human Resources Policies and Practices (hiring, evaluations and continuous education)
- **Customer onboarding, maintenance and offboarding**
- **Personnel management**
- **Maintaining payroll master files**
- **Recording time**
- **Calculating payroll**
- **Disbursing payroll**
- **IT (Infrastructure, Applications, Security, Operations and Change)**

Managed IT / IaaS

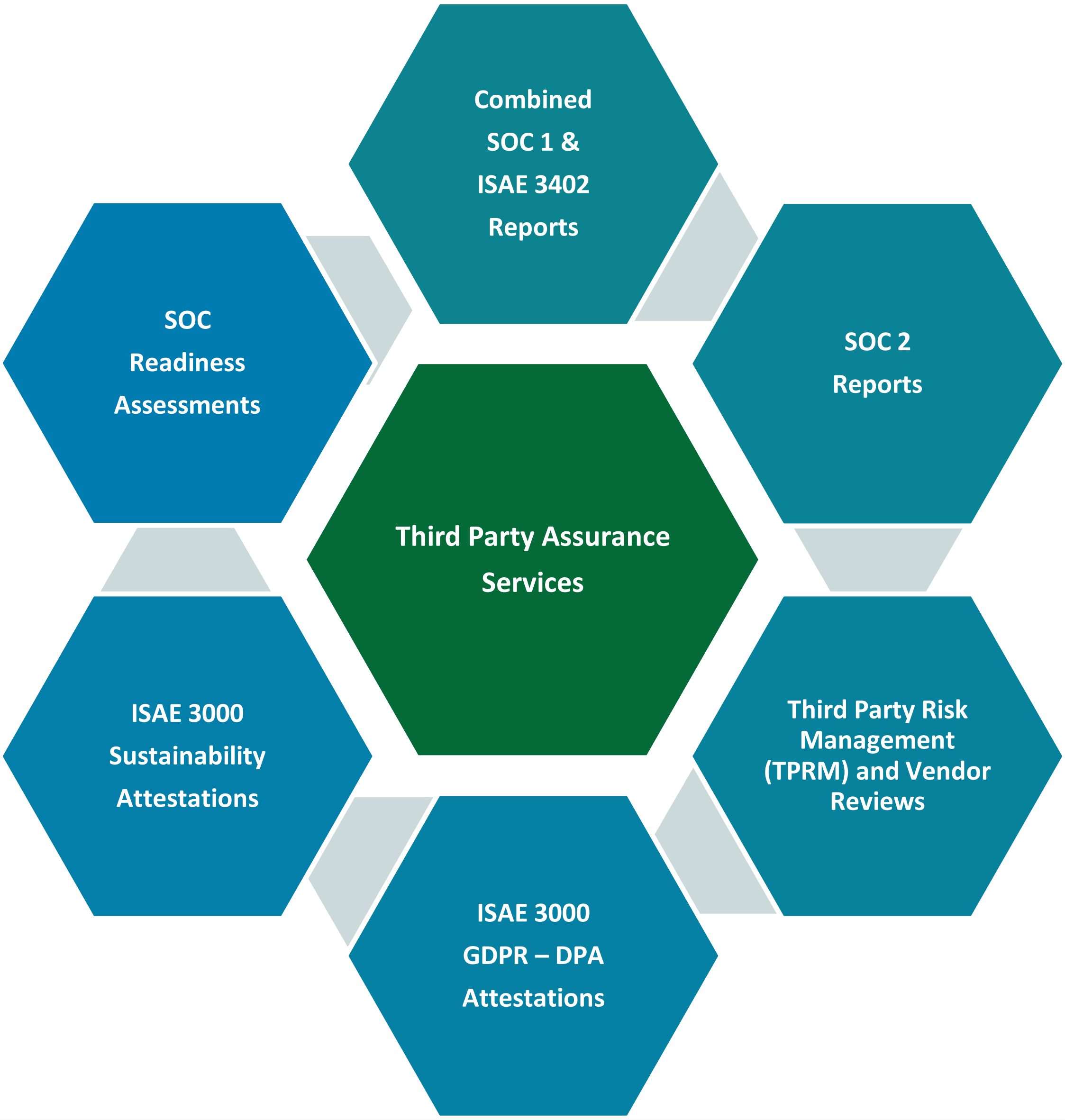
- **Control environment, risk assessment and monitoring**
  - Corporate Governance
  - Risk Management and Internal control
  - Organizational Structure
  - Human Resources Policies and Practices (hiring, evaluations and continuous education)
- **Customer onboarding and offboarding**
- **Information Security (logical access to programs, data, and computer resources as well as physical access to computer and other resources**
- **Change Management over changes to application programs and related data management systems**
- **Network infrastructure configuration**
- **Computer Operations in regard to the execution and monitoring of application and / or system processing and data transmissions**
- **Backup and recovery**
- **Incident management and managing customer queries**
- **Problem management**
- **Subservice provider governance and monitoring**

Software as a Service (SaaS)

- **Control environment, risk assessment and monitoring**
  - Corporate Governance
  - Risk Management and Internal control
  - Organizational Structure
  - Human Resources Policies and Practices (hiring, evaluations and continuous education)
- **Customer onboarding and offboarding**
- **Information Security (logical access to programs, data, and computer resources as well as physical access to computer and other resources**
- **Change Management over changes to application programs and related data management systems**
- **Computer Operations in regard to the execution and monitoring of application and / or system processing and data transmissions**
- **Backup and recovery**
- **Incident management and managing customer queries**
- **Problem management**
- **Subservice provider governance and monitoring**

Deloitte’s ISAE3402 Services

Deloitte’s Third-Party Assurance Services


Combined SOC 1 & ISAE 3402 Reports
SOC 2 Reports
Third Party Risk Management (TPRM) and Vendor Reviews
ISAE 3000 GDPR – DPA Attestations
ISAE 3000 Sustainability Attestations
SOC Readiness Assessments
Third Party Assurance Services

We have experience in providing the following Third-Party Assurance services:

- **SOC1 & ISAE 3402 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.

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

- **ISAE 3000 Data Processing Agreement Attestation (GDPR Compliance)** – we provide attestations to customers which are used to evidence compliance with the terms outlined in their Data Processing Agreements.

- **Third Party Risk Management (TPRM)**– assisting clients in formalizing their third-party risk evaluation and mitigation efforts, including methods to inventory third-party relations, classify the risk of each existing and any future third-party relations, developing self-assessment questionnaires for covering varying risk themes (e.g., cyber, financial, climate and sustainability), methods for reviewing responses and defining and executing audit procedures necessary resulting from the assessments.

- **Vendor Reviews** – using our vast experience in both auditing and assisting vendors with their internal control needs, we can perform reviews of your vendors for you to provide you with assurance for specific risks you have identified or just follow one of our specific vendor audit programs for specific topics.

- **Sustainability Reporting attestation** – we provide attestation reports on companies’ sustainability reporting as well as other Climate and Sustainability related topics.

- **SOC Readiness Assessments** – We perform gap analyses and readiness assessments for all of the above topics.

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

Deloitte 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.

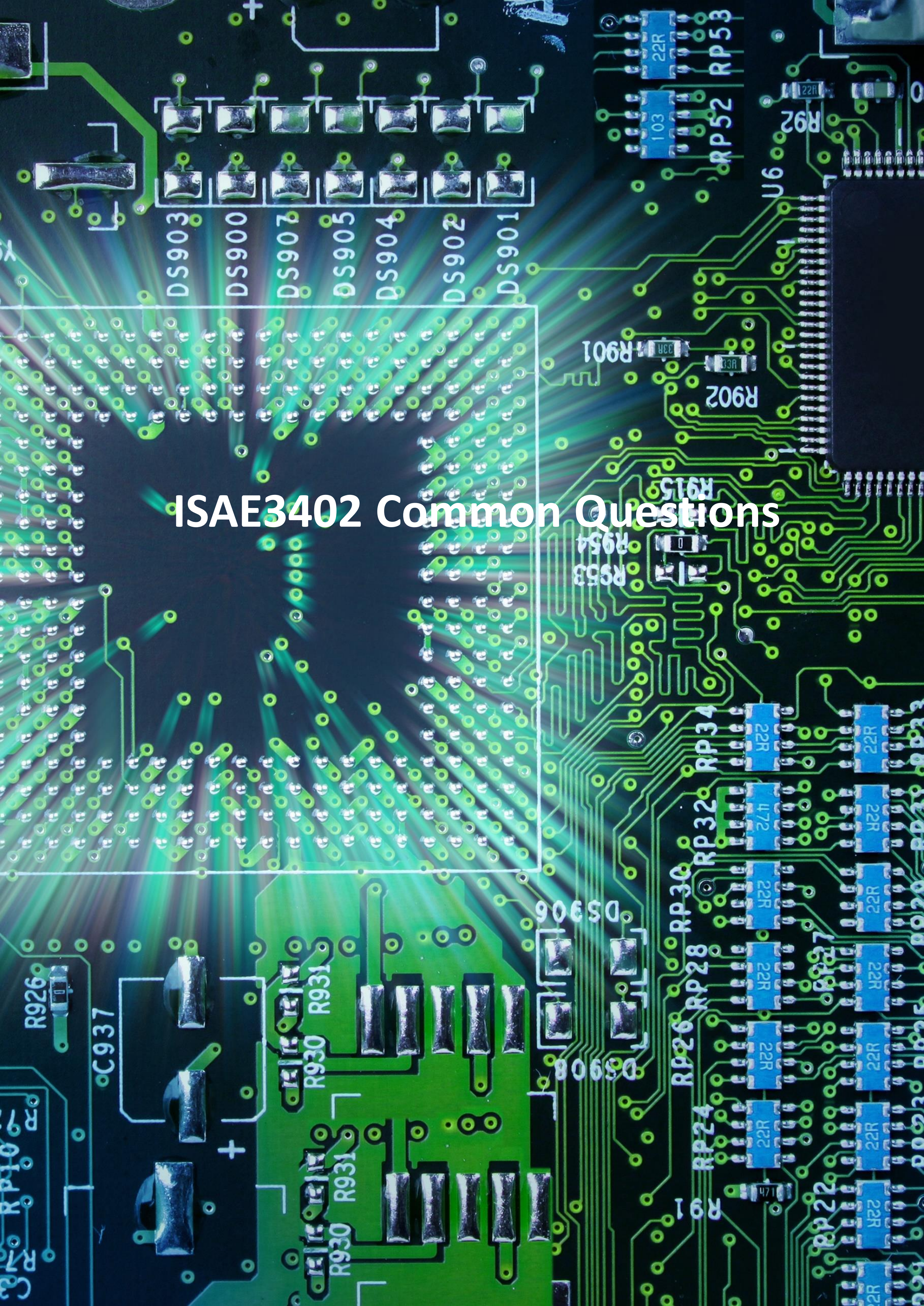
The following is a list of some of the engagements our Norwegian Team has worked on or are currently delivering. We support engagements across the Nordic region, as indicated (NO, SE, DK).

- **Payroll processing** (ISAE3402 Type 2 - Payroll)
- **SaaS provider** (SOC 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** (SOC2 Type 2 – IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS) (DK)
- **Transportation services** (ISAE3402 Type 2 – Ticket income distribution)
- **IT services** (SOC2 Type 2 – IT) (DK)
- **Financial services** (ISAE3402 Type 2 – IT) (DK)
- **Educational Institution** (ISAE3402 Type 2 and ISAE3000 GDPR (DK)
- **SaaS provider** (SOC2 Type 2 - SaaS)
- **Financial services** (ISAE3402 and multiple SOC2 reports – Financial services) (SE)
- **IT services provider** (ISAE3402 Type 2 – Managed IT)
- **SaaS provider** (ISAE3402 Type 2 – SaaS)
- **IT security services** (SOC2 Type 2 – IT Services)
- **Airline** (ISAE3000 Type 1 – Process integrity)
- **SaaS provider** (SOC2 Type 2 – SaaS)
- **SaaS provider** (SOC2 Type 2 – SaaS)
- **IT services** (SOC2 Type 2, ISAE3402 Type 2 and ISAE3000 GDPR – Managed IT))
- **Financial services** (SOC2+ with CSA CCM – Financial services) (DK)
- **SaaS provider** (ISAE3402 Type 1 – SaaS) (DK)
- **SaaS provider** (SOC2 Type 2, ISAE3000 GDPR and ISAE3000 for MitID and NSIS - SaaS)
- **IT services provider** (ISAE3402 / SOC1 combined and SOC2 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.

ISAE3402 Common Questions



Some common questions

What are my options for design of the report?

We are focused on providing our customers with a product they can be proud of and which represents the hard work behind what we do. That being said, these reports are sometimes large (over 100 pages) and publishing them takes time. We use Word and Excel in most reports and try our best to format them in a professional manner. If you would like to involve your own marketing department, for example, to assist in the design of the report, you would be free to do so. We should be informed of this as soon as possible in the attestation process as the design of the report should not delay the actual distribution date of the final attestation.

Also. We generally provide electronically signed PDF versions of the report. If special PDF versions are necessary or if you would like physical print versions of the report, please also let us know as soon as possible.

What are my options for distribution of the report?

You are free to distribute the final and signed version of the report which we send to you to whichever customers (and / or their external financial auditors) and prospective customers you like. You will not be able to publish the report on your web page or extract portions of the report for distribution. The report needs to be distributed in its entirety to enable the receivers to have the full context available to them. Also, you are required to be able to provide us with a list of the receivers of the report upon request.

Are there any logos or such that I can use for my attestation?

The AICPA has its own special requirements in regard to the use of the various logos they have. You will need to go to their home page to download logos directly and to check the latest updates to their requirements. This applies to the SOC 1 and SOC 2 reports. The ISAE3402 and ISAE3000 are under international guidelines and we are not aware of any specific rules about these at this point.

An extract of the introduction text from the AICPA Guidelines at this time is as follows:

> *The official AICPA SOC for Service Organizations – Service Organizations logo (the "SOC for Service Organizations – Service Organizations Logo") is provided herein. The SOC for Service Organizations - Service Organizations Logo is owned by the American Institute of Certified Public Accountants ("AICPA"). The AICPA has established the following guidelines (the "Guidelines") that govern your display and use of the SOC for Service Organizations - Service Organizations Logo. In order to download and use the SOC for Service Organizations - Service Organizations Logo, you will be required to complete and submit the registration page, by which act you are affirming that you have read, understand and agree to comply with these Guidelines.*

This guidance can be found here:

https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-service-organizations-logo-guidelines-cpa.pdf

Deloitte ISAE3402 Contacts

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

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.