Swiss ISAE & SOC Readiness Study 2025

KPMG Switzerland

KPMG. Make the Difference.

November 2025

Study purpose

This first-of-its-kind study in Switzerland examines the use and impact of ISAE/SOC reports across industries and regions, focusing on their content, global distribution and the way ISAE processes are implemented, practiced and perceived internally.

Swiss companies with both local and global operations face diverse regulatory requirements, including FINMA circulars, EU directives and SEC rules. As a result, a growing range of sectors, such as Technology, Real Estate and Healthcare, now demand ISAE/SOC reports. Emerging regulations, such as the EU-Cyber Resilience Act, may further shape the ISAE/SOC landscape.

The analysis shows that regulatory compliance is often the primary driver for adopting these reports. However, integrating controls into operational processes can reduce administrative effort and enhance business value. These insights aim to help companies optimize their related processes and get the best value out of their ISAE/SOC reports.

Stefan Wälti
Partner,
Head of Assurance Technology
KPMG Switzerland

Main learnings

ISAE/SOC reports play a critical role for meeting regulatory obligations while strengthening market credibility. The main challenges lie in the quality of documentation, limited automation and the need for effective collaboration. Innovations, particularly AI-driven solutions and advanced tools, are viewed as critical enablers for further optimization.

01 The **primary purpose** of ISAE/SOC reports **remains regulatory compliance**. Beyond that, they also create opportunities for **market growth** and competitive differentiation.

02 **ISAE 3402 reports dominate** the Swiss market, accounting for nearly 50% of all reports. ISAE 3000 follows with 25%, while **SOC 2 is steadily gaining traction** at 18%.

03 The **number of controls varies** across frameworks, averaging 44 per report. Most **controls are still manual**, requiring between one and five hours to execute each.

04 **Challenges** in the ISAE/SOC process often stem from **frequent turnover** among control owners and auditors. Key issues include **inconsistent quality** of evidence, while **collaboration with auditors** remains resource-intensive and **could be improved**.

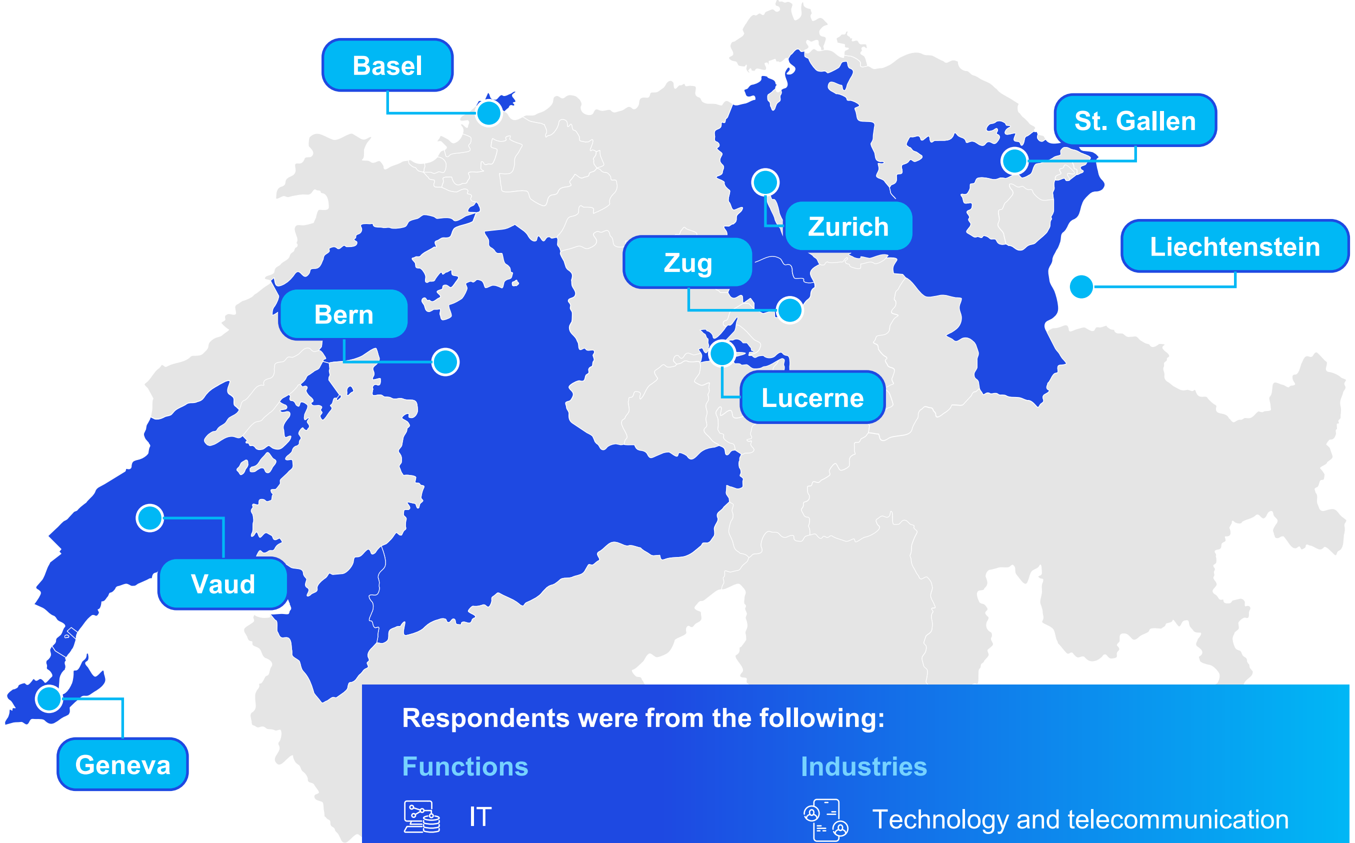
05 The **impact** of **Artificial Intelligence** (AI) is still **uncertain**. However, there is **strong optimism** that AI could significantly improve efficiency in evidence collection, monitoring, and outlier detection.

06 **Best practices** for companies establishing reports include integrating **Governance, Risk & Compliance (GRC) tools and automation** early in the process. A **clear strategy** and defined ownership are essential to implement **risk-oriented**, practical **controls** effectively.

Study overview

27 participants across **5** industries in Switzerland.

4 expert interviews



Respondents were from the following:

Functions

- IT
- Risk & Compliance
- Finance
- Information Security
- Process Management

Industries

- Technology and telecommunication
- Financial services and insurance
- Government
- Construction and real estate
- Software services

Contents

01 Organizational insights

02 Reports insights & focus topics

03 Controls & processes

04 Impact of AI & AI Assurance

05 Outside-in view

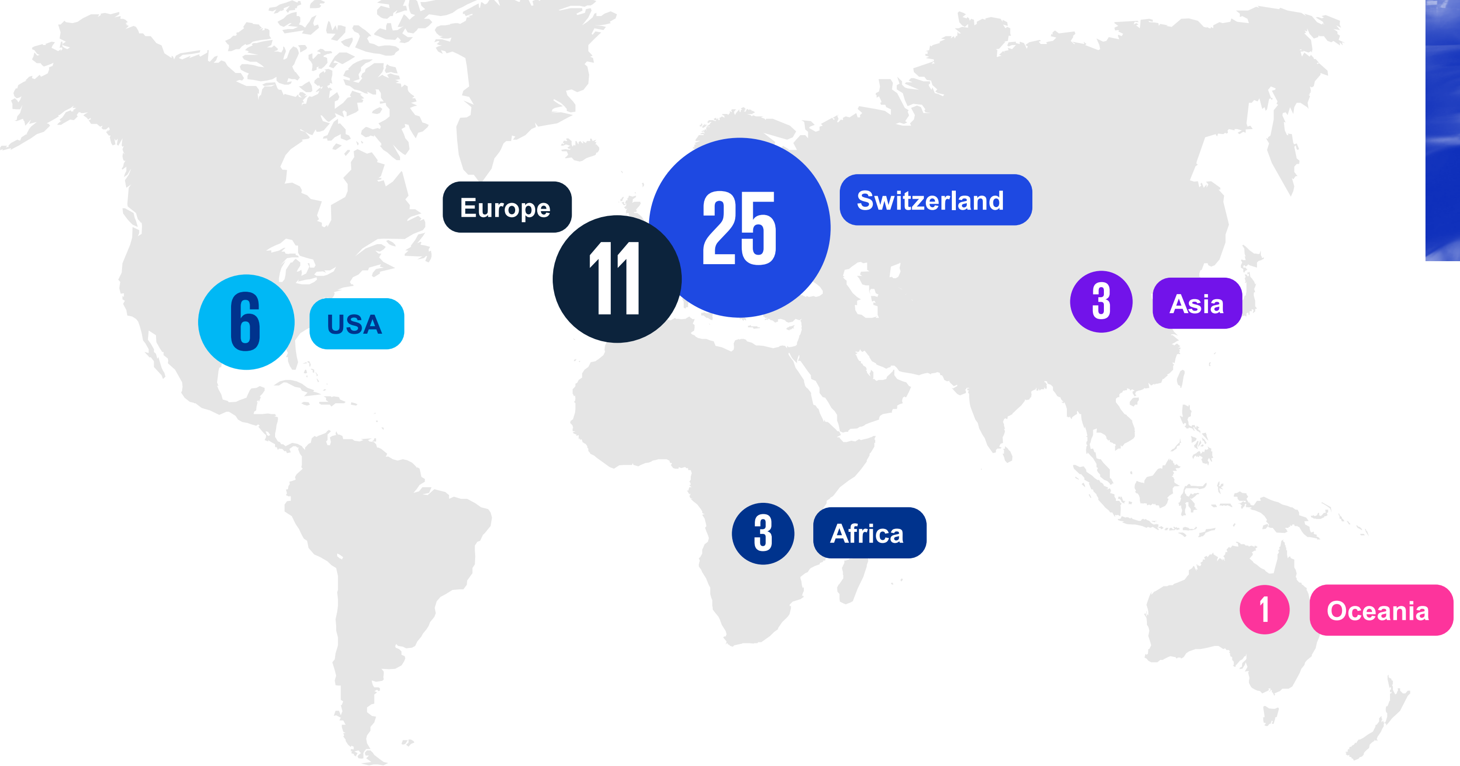
06 Outlook & recommendations

Organizational insights

01

Where are ISAE/SOC reports used globally?

Reports by region: distribution across all study participants



Companies participating in the study primarily issue reports for the Swiss and broader European markets.

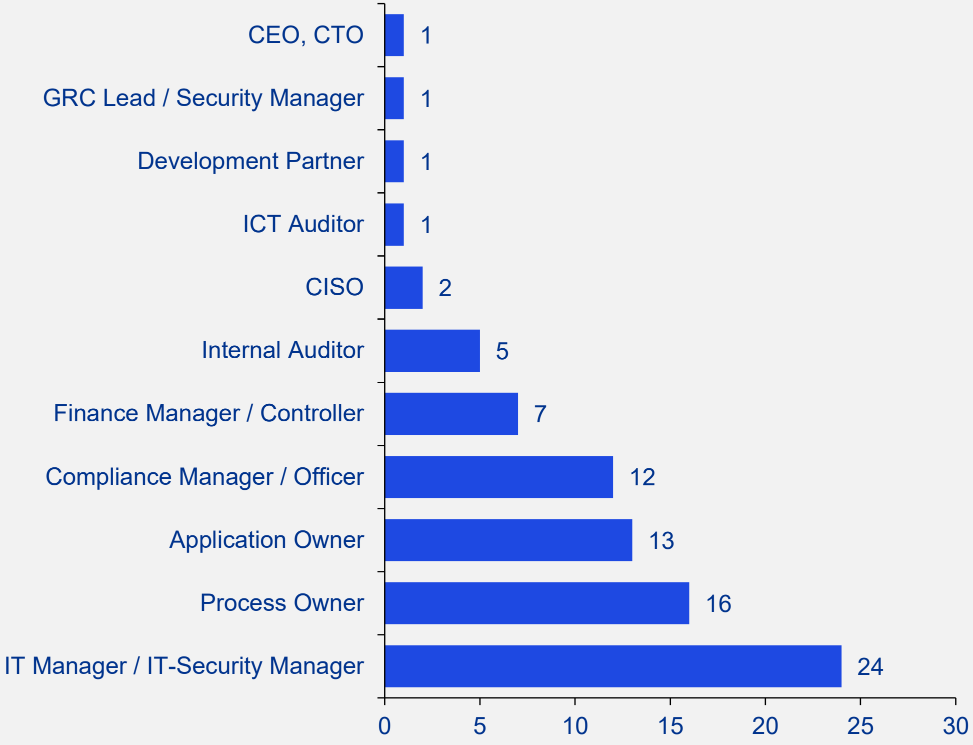
Those operating on a global scale – especially in the Technology, Media and Telecommunications sector – are the most likely to publish internationally.

Organizations expanding beyond Switzerland and Europe often adopt ISAE/SOC reports to meet international compliance requirements and build trust in new markets.

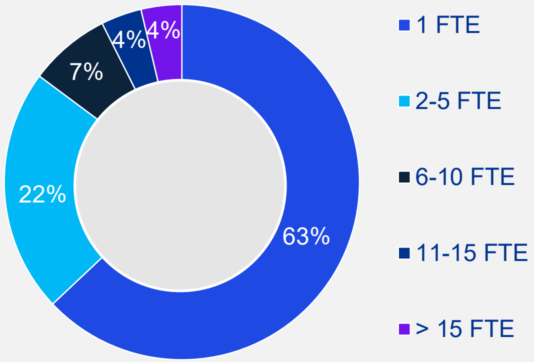
Recent requests for proposals confirm that these reports are increasingly viewed as essential for market entry.

Organizational insights and ISAE/SOC processes

Which roles (job titles/functions) are involved in the ISAE/SOC process?

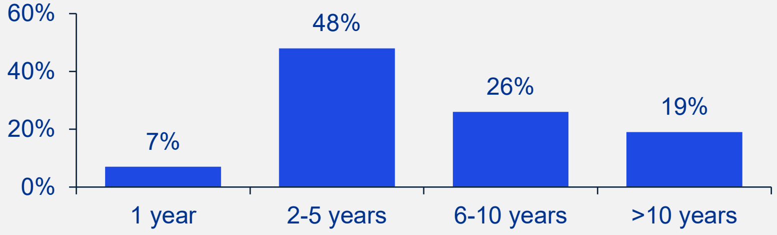


How large is the team responsible for preparing ISAE/SOC-related activities in FTEs?



In smaller and mid-sized companies, only a fraction of an FTE is typically allocated to manage the ISAE/SOC process.

How long has your ISAE/SOC reporting been in place?



41% of the respondents are updating their ISAE/SOC framework on an annual basis.

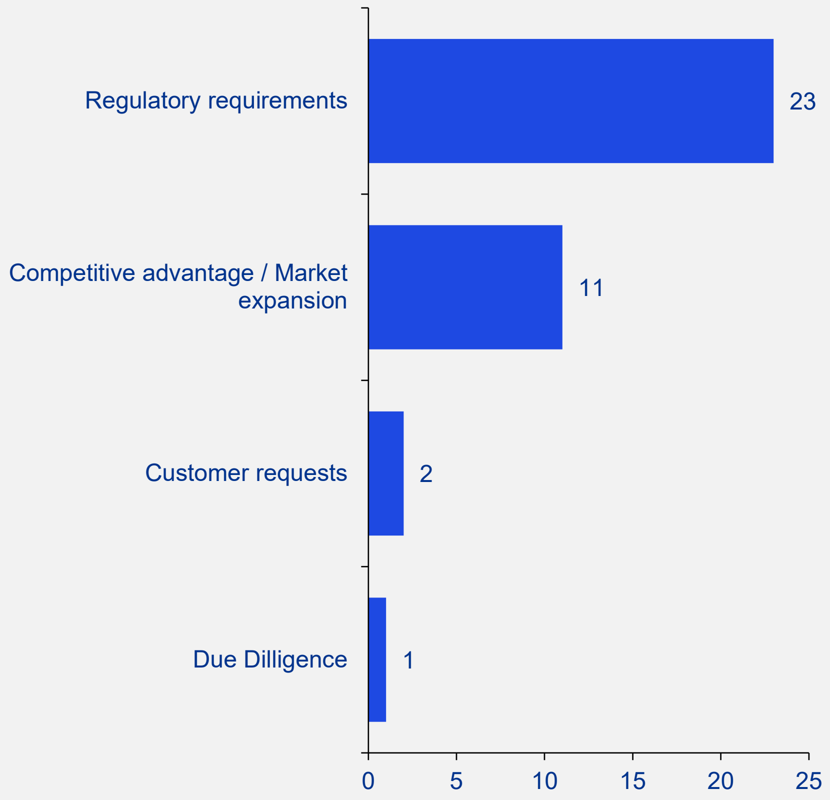
48% are performing the update on demand, based on regulatory requirements.

11% of the respondents have no formalized ISAE/SOC process.

In two-thirds of cases, companies collect innovations through continuous improvement processes, centralized ideation and lessons-learned workshops. One-third of companies currently have no formalized innovation process in place.

Organizational insights and ISAE/SOC processes

Reasons for establishing the ISAE/SOC report



70% operate with both standardized and manual processes

Companies' self-assessments of ISAE/SOC maturity show that **nearly 70% rate their processes and controls as standardized but mostly manual**. Around 20% consider their processes well-integrated and largely automated, often supported by GRC tools or benefiting from more than a decade of experience.

Excel and SharePoint are used alongside other GRC tools

Excel and SharePoint remain the primary tools for managing ISAE processes. Expert interviews reveal that integrating specialized solutions into existing IT landscapes is often challenging. However, this value proposition may shift as IT environments evolve.

Beyond ServiceNow, Confluence, Jira, and Archer, tools such as Vanta or Workiva were not mentioned by participants. Notably, **one in five companies indicated plans to implement a new tool** to support the process in the future.

Companies market reports through websites mostly

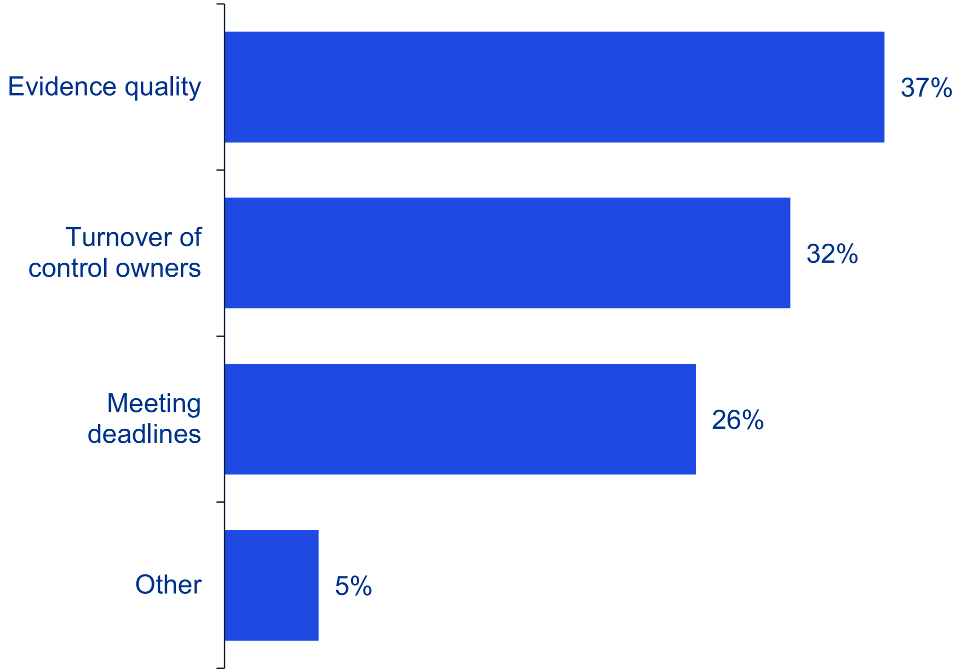
The study shows that **most companies feature their ISAE/SOC reports on their websites** alongside certifications such as ISO 27001. These reports are commonly **used in tenders and due diligence projects** and are often offered as an added service for clients.

Biggest challenges in the ISAE/SOC processes

37%

of participants identified **quality of evidence** as one of the **biggest challenges**, followed by turnover of control owners (32%). Expert interviews confirm these as key pain points.

Meeting deadlines is a related issue, cited by one in four companies, with delays often linked to coordination between companies and auditors. Additionally, 5% noted that changing auditors during the testing phase creates further complications.

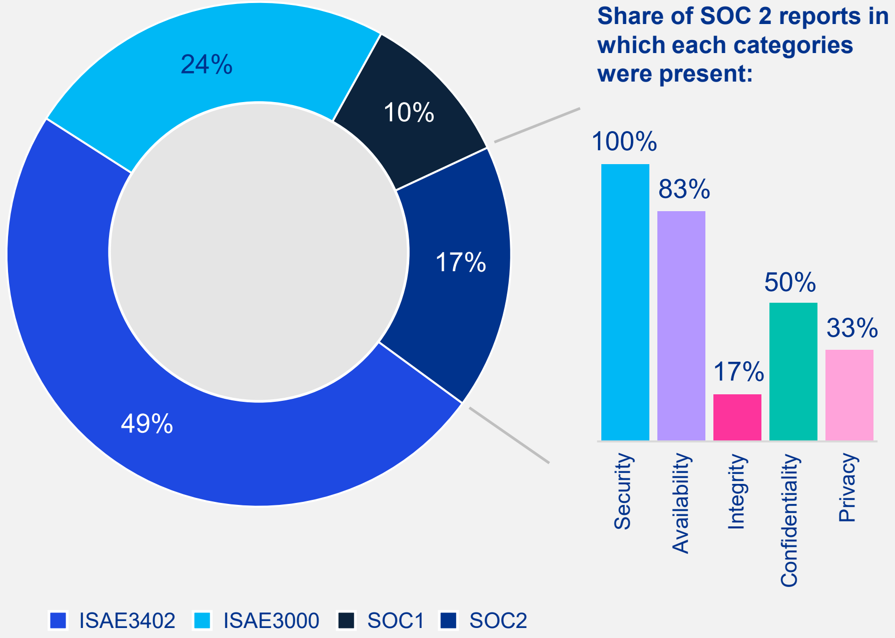


Report insights & focus topics

02

Report insights

Report standards



Share of SOC 2 reports in which each categories were present:

2 out of 27 respondents reported that their reports were qualified (7%). By comparison, a recent UK benchmark shows 20% of reports were concluded as qualified.

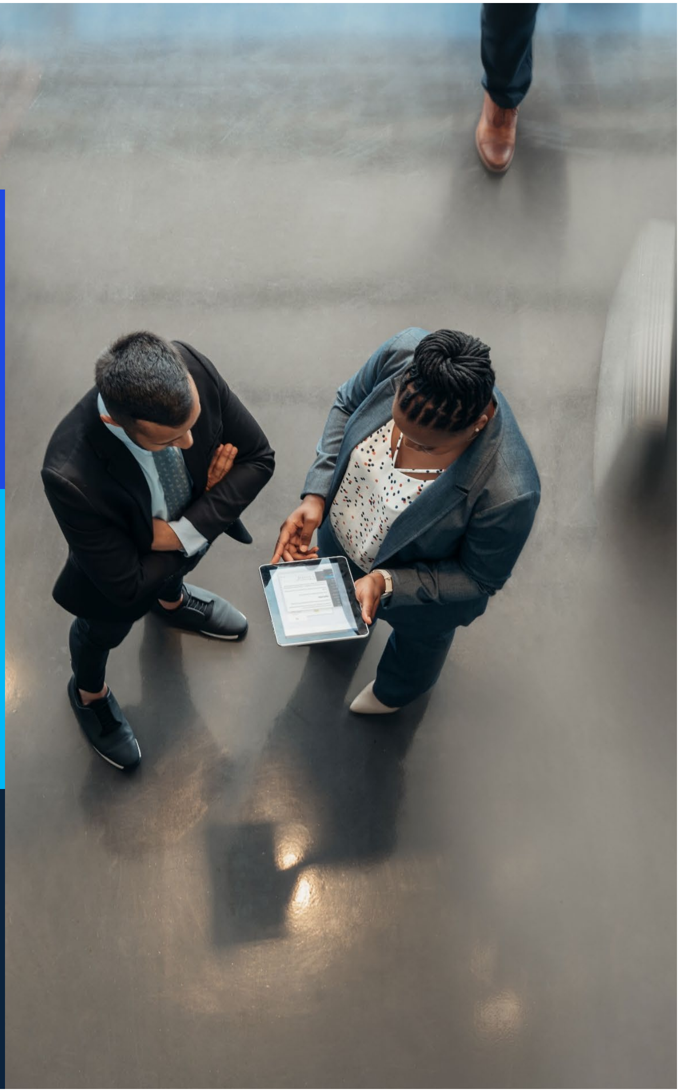
Most participants exclude third-party suppliers using the carve-out method.

Only **7 out of 26** of companies apply the inclusive method.

On average, reports include

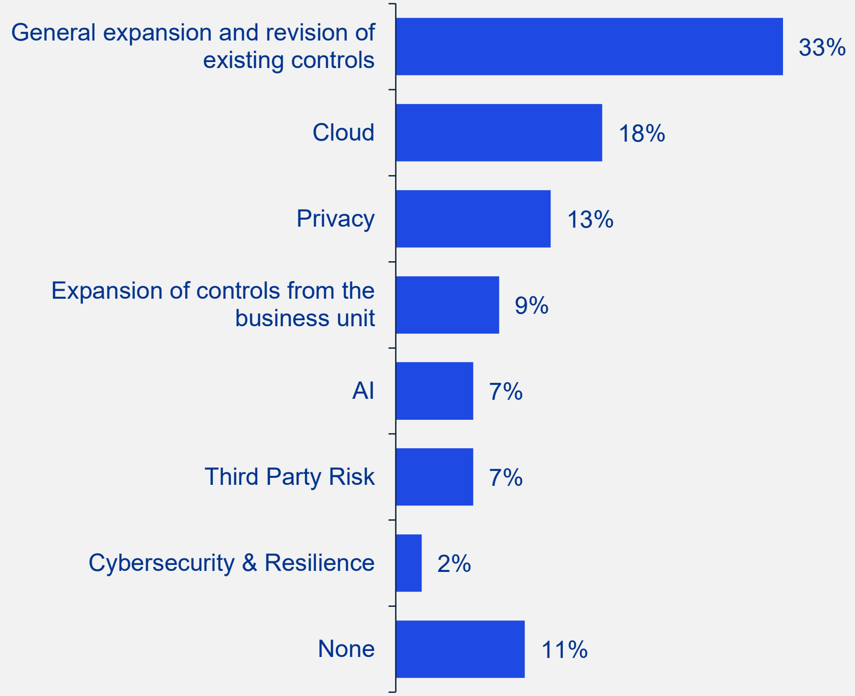
44 controls.

ISAE 3402 and ISAE 3000 reports typically have around 37 controls, while SOC 2 averages 85 controls per report.

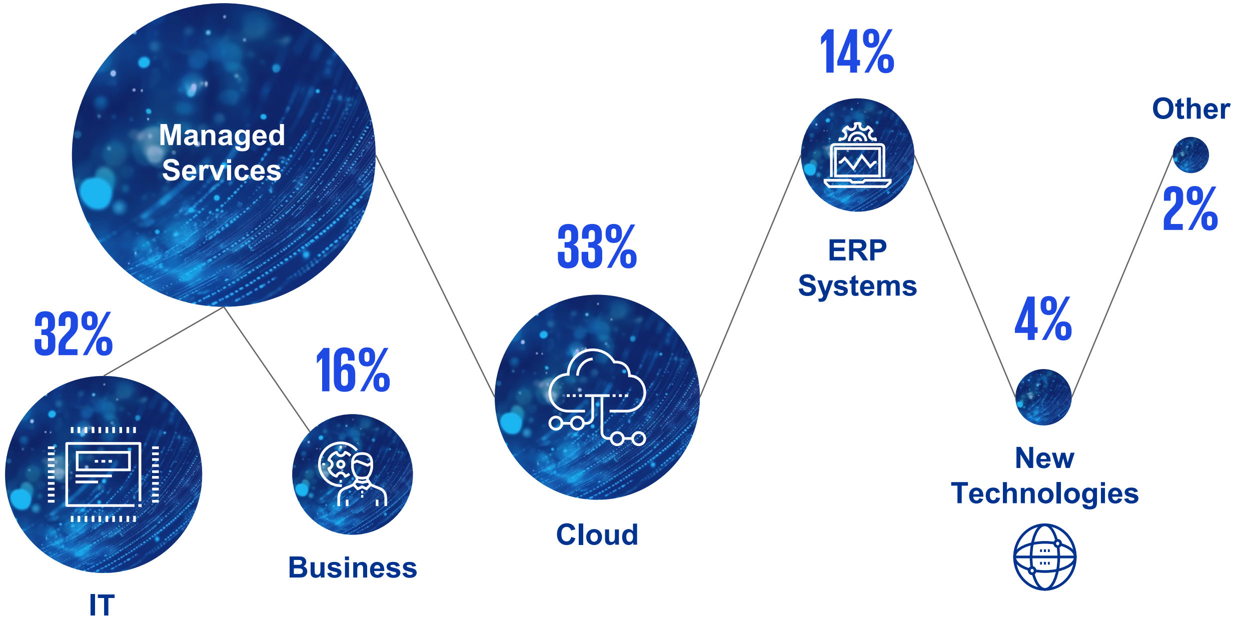


Report insights

Which subject areas have been added in the past 1-3 years?



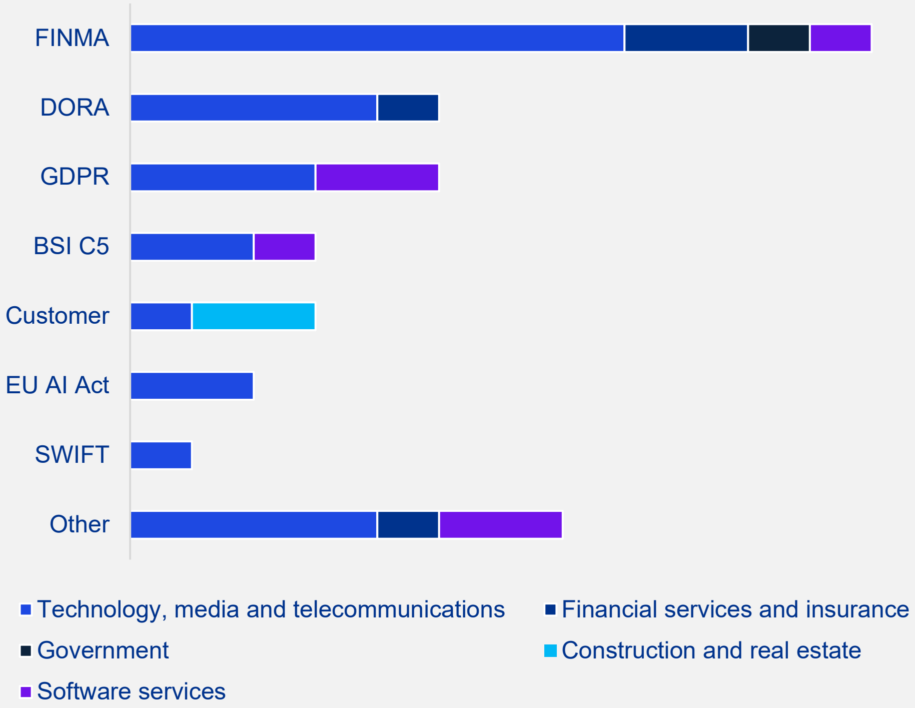
Which subject areas are covered by the reports?



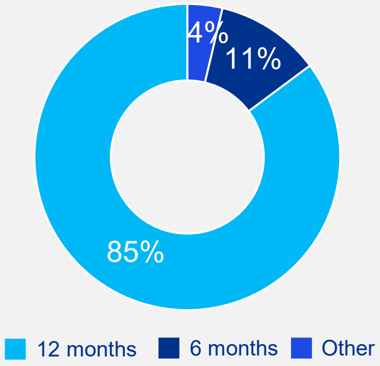
Companies are transforming their businesses by modernizing processes and underlying systems. This shift from on-premise to cloud-based solutions **has driven a rising demand for ISAE/SOC reports**. At the same time, reliance on managed services is increasing, often influenced by customers' Internal Control Systems. **Looking ahead, reports** related to emerging technologies are expected to place **greater emphasis on Artificial Intelligence**, with stronger focus on governance and model oversight. Notably, KPMG is among the first firms preparing to issue a SOC 2+ report covering AI.

Report insights

Requirements that are addressed through the issuance of the reports.



85% of reports cover 12 months, while 11% cover 6 months and 4% another period (mostly in the context of first-year reports).



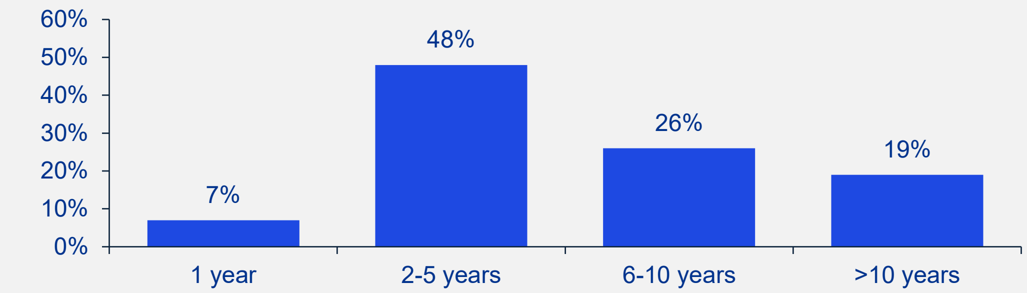
Unsurprisingly for Switzerland, nearly half (44%) of respondents indicated that **FINMA requirements are the primary driver for issuing reports**. Additionally, other EU regulations, particularly from the financial services and healthcare sectors, are also addressed. About 17% of respondents stated that their reports address **external audit requirements and specific industry standards**.

Expert interviews revealed that all interviewees unanimously agreed on the importance of adding **value to the business, rather than treating reporting as just a compliance task.** To achieve this, early communication and strong collaboration between business, IT and compliance teams are essential.

Regarding reporting periods, a **12-month cycle is the standard in Switzerland**, reflecting the fact that most companies close their financial year on 31 December. However, companies in the Real Estate sector, as well as some in the technology, media, and telecommunications industries, often issue reports covering a six-month period.

Report insights

How long are your ISAE/SOC reports in place?

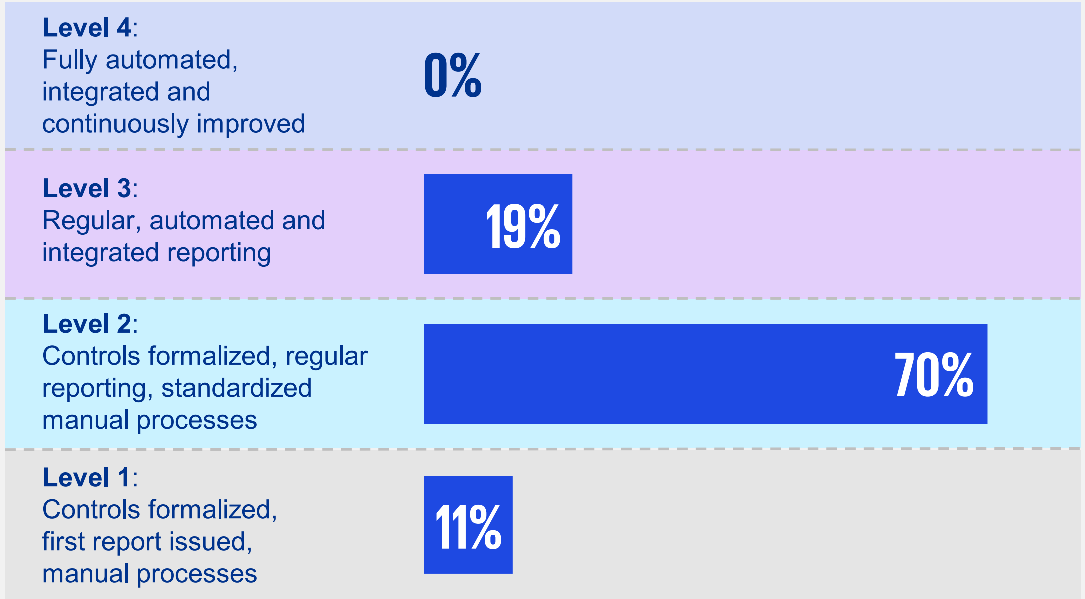


The study revealed that **55% of participating companies issued their first ISAE/SOC reports within the last five years.** Among these, 81% assess their ISAE/SOC process maturity on the lower end. Overall, 23% are planning to introduce a tool supporting these processes in the next 12 months to increase maturity.

Insights from expert interviews and recent request for proposals indicate that **companies that are newer to ISAE/SOC reporting often prioritize automation from the outset**. In contrast, more **mature organizations** tend to **adopt automation** and process improvements **more gradually**.

Particularly **start-ups and scale-ups aim** to embed automation and controls early, with the ambition of achieving **higher maturity** from the start.

Maturity of ISAE/SOC process



Controls & processes

03

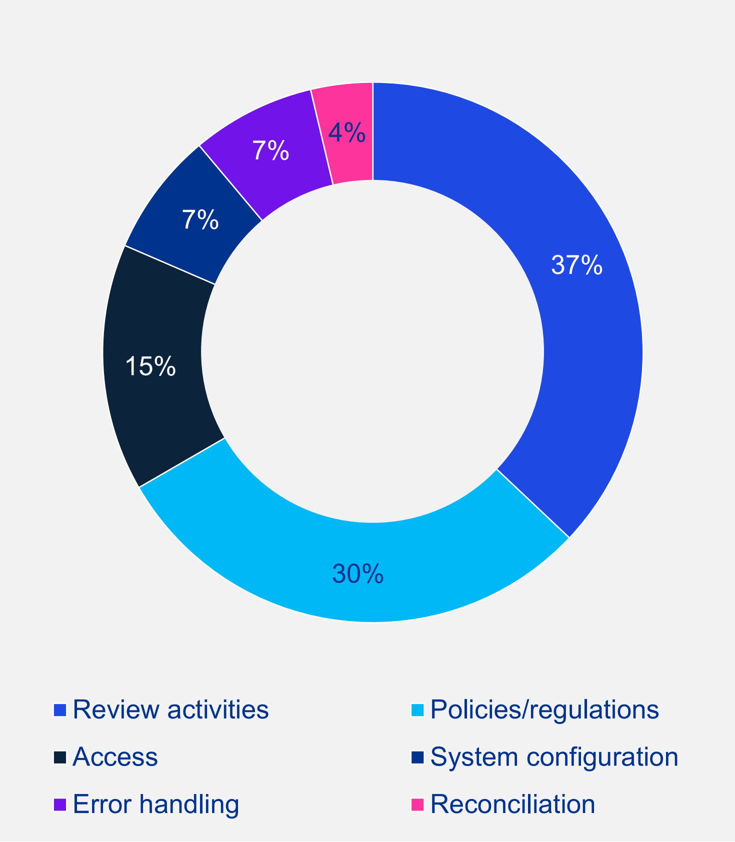
Control insights

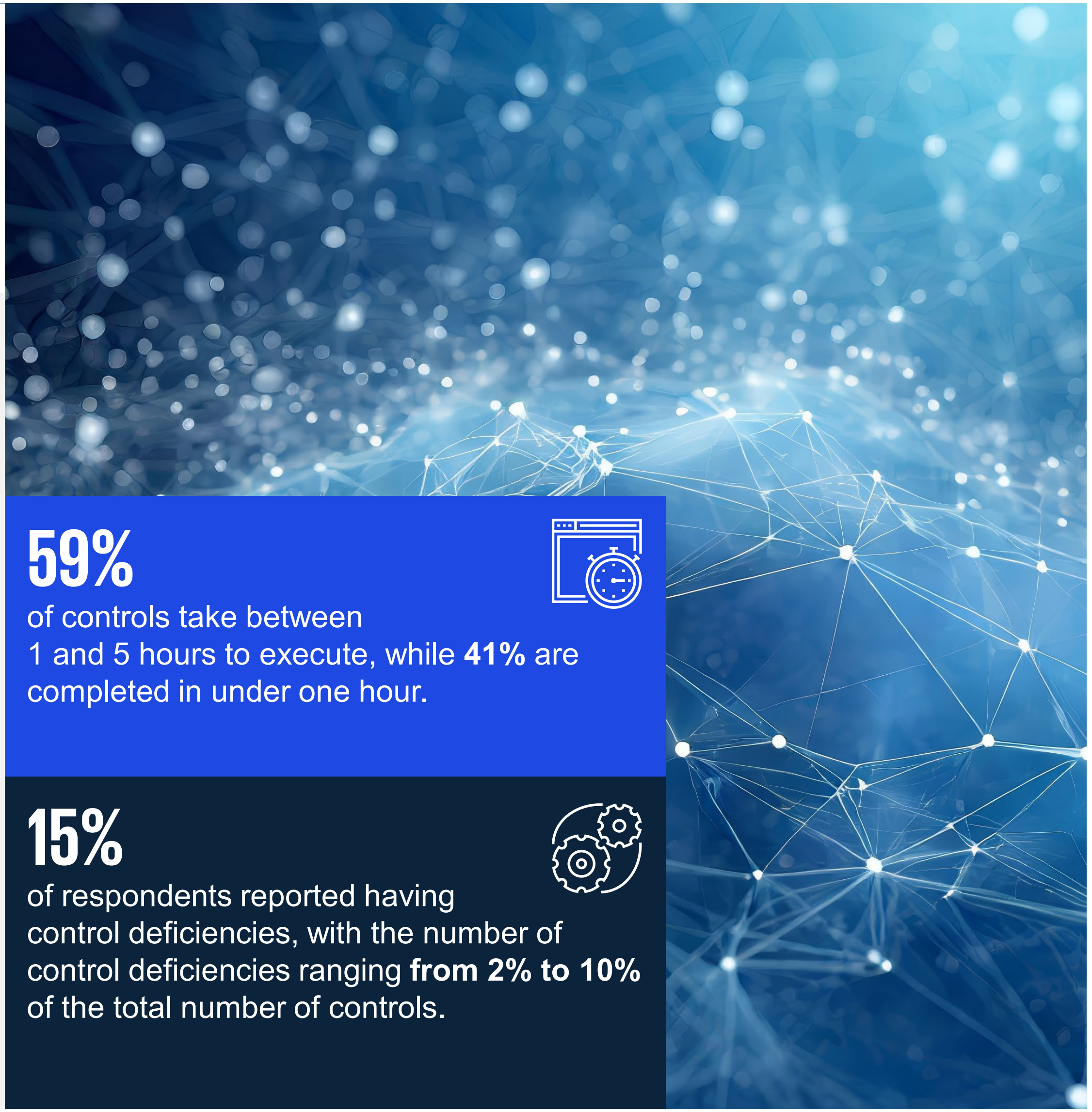
37%

of controls are related to **review activities, followed by 30% related to policies** and procedures, and 15% to system access.

System configuration and error handling controls each account for 7%, while reconciliation controls make up 4%.

Review activities and policies / procedures were identified as the areas with the **greatest potential for improved efficiency.**





59%

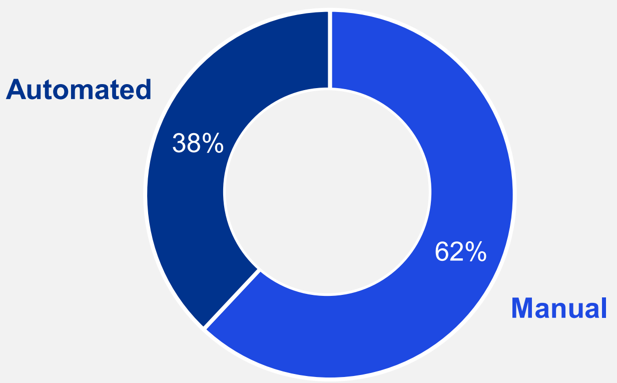
of controls take between 1 and 5 hours to execute, while **41%** are completed in under one hour.

15%

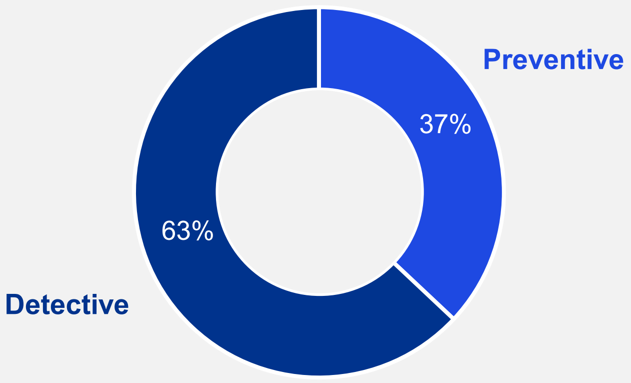
of respondents reported having control deficiencies, with the number of control deficiencies ranging **from 2% to 10%** of the total number of controls.

Control insights

Control nature



Control type



62%

of controls are manual in nature, with **some organizations having only manual controls.** This confirms the **need for more automation** in the operation of controls.

63%

of controls are classified as **detective**. Such controls tend to **be less robust and more time-consuming**, which increases both the risk of failure as well as the cost of operating the control.

These statistics once again **highlight the need for greater automation.**

Impact of AI and AI Assurance

04

Navigating AI’s role in ISAE/SOC audits

Companies, particularly start-ups and scale-ups, are enhancing their solutions with Artificial Intelligence (AI) to help end customers become more effective. In contrast to AI-powered products, most study participants cannot yet fully assess the impact of AI on the ISAE process and its controls.

AI as a driver

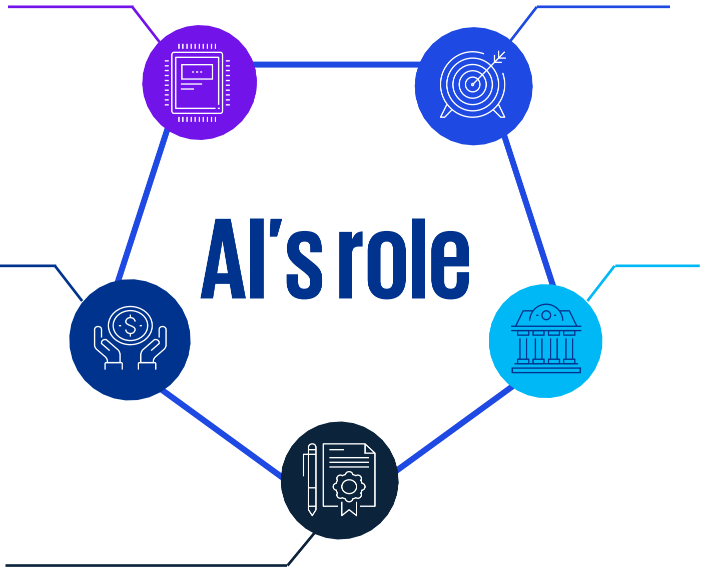
- Management expects **results with maximal business impact**
- Availability of new AI tools and platform **facilitates access to technology**

Expected benefits

- **Facilitates collection** of audit evidence (e.g., screenshots)
- Supports monitoring activities and **anomaly/outlier detection**
- Accelerates shift towards continuous, **data-driven compliance**

Outcome, quality & human oversight

- AI results **depend on multiple parameters** (e.g., training data)
- **Uncertainty** around **what can be assured** from AI-generated outcomes
- **Human validation still necessary** to ensure expected quality (Human-in-the-loop concept)



AI’s role

Current challenges/hurdles

- Lack of a **clear vision** for AI’s role in ISAE/SOC audits
- **Audit requirements** often mandate human execution of controls
- New risks introduced by AI-driven processes

Governance, assurance & transparency needs

- **Clear rules and governance** frameworks required
- Need for explainable, safe and reliable AI processes
- Solutions/products are supercharged with AI; **AI is often treated as a “black box”**
- Assurance focus will **shift over time** from the underlying security layer **to models and output**.

How to achieve Assurance of AI?

Achieving assurance over AI systems is an ongoing journey, structured into eight key steps:

01 **Implement an AI strategy & governance framework for responsible AI usage**

Develop and formalize an AI strategy and governance framework that align with relevant regulations and ethical standards.

02 **Inventory and categorize the current AI landscape by risk**

Identify all AI systems in use, evaluate their purpose and assess their associated risk level.

03 **Conduct a gap analysis to identify areas of non-compliance**

Compare current AI practices against regulatory and internal requirements to pinpoint areas of non-compliance.

04 **Automate model management and evaluation to ensure compliance**

Continuously monitor AI models for accuracy, fairness and bias using automated tools, and trigger alerts for any deviations.

05 **Perform a data privacy and security review and update as needed**

Regularly audit data protection measures to ensure compliance and safeguards against unauthorized access or misuse.

06 **Maintain inventory of AI systems to ensure traceability and ongoing monitoring**

Keep an up-to-date inventory of all AI systems and monitor them for emerging risks or issues.

07 **Train employees on AI ethics and compliance**

Educate staff on ethical AI use, potential biases and organizational policies to foster responsible practices.

08 **Attestation engagement**

Independent attestation report over AI setup, gives objective feedback, and builds trust by confirming responsible AI use.

Outside-in view

05

Expert interviews

To validate the study findings and further explore key topics, four expert interviews were conducted, offering practical insights into how organizations approach ISAE/SOC reporting. Here is our summary:

- A major insight is that **preparation for the audit is a critical success factor**, particularly in complex environments or scenarios involving multiple reports. Dedicated teams conduct selective control checks throughout the year to ensure that controls operate with the appropriate quality and parameters.
- A more detailed but **important aspect** of ISAE/SOC audits is ensuring **Completeness & Accuracy (C&A) in sample populations and review controls**. Experts identified **significant potential for automation** to streamline this process. Recording control execution can also help demonstrate C&A and support review steps, especially when evidence is time-sensitive.
- Experts also reflected on the early phases of the ISAE journey and emphasized that a **readiness assessment or mentorship model would have been helpful to get off to a strong start.**
- Such an approach would support organizations in establishing a fit-for-purpose control framework and an end-to-end ISAE/SOC process from the start, resulting in reduced overhead and added value.
- Another recurring theme was the importance of **clear guidance and expectation-setting from auditors**, such as defining minimum control requirements or approaches for handling exceptions. Having the right **auditor with relevant experience** and a client-centric mindset was described as **critical for success**.
- In terms of innovation, experts highlighted the need for **close collaboration between business and ISAE/SOC teams** to ensure that product innovations are appropriately reflected in control designs and reports.
- The interviews also revealed that once a company has issued an ISAE/SOC report, it becomes challenging to discontinue or adjust it, as both customers and the market begin to expect the report on an ongoing basis. Experts recommended **periodically reviewing the trade-off between customer contractual agreements and the organization’s actual business needs**.

Key insights

- Conduct readiness assessments early to prevent inefficiencies later.
- Invest in building awareness and internal knowledge of ISAE requirements.
- Automate the collection of Completeness & Accuracy evidence wherever possible.
- Ensure clear communication and alignment of expectations with auditors.
- Periodically reassess the need for an ISAE report, particularly after changes in customer or regulatory requirements.

Where lies the biggest demand for innovation?

Automation & efficiency

- **Organizations view automation as the most critical driver for innovation.** It focuses on reducing manual tasks such as evidence collection, control execution and report preparation.
- **Digitalization through GRC** platforms and workflow tools facilitates faster audits, **reduces human error** and improves overall efficiency.

Integration & harmonization

- Companies aim to **integrate different systems** (audit platforms, documentation tools, compliance dashboards) to **create a seamless data flow and synergies.**
- **Standardizing processes** and harmonizing controls **across frameworks** like ISAE, SOC, and ISO 27001 helps reduce complexity and ensures scalability for global operations.

User experience & collaboration

- Innovation is not just about technology but also usability. Participants highlighted the **importance of intuitive, user-friendly tools** that simplify compliance tasks for control owners and auditors.
- Enhanced collaboration features, such as **real-time dashboards** and transparent communication channels, improve **trust and efficiency between auditors and organizations**.

Data analytics & AI

- Advanced analytics and AI are expected to **shift compliance from a reactive to a proactive approach**. They enable anomaly detection, predictive risk analysis and continuous monitoring.
- AI-driven insights can help organizations **prioritize controls,** allocate resources more effectively and **improve quality of audit evidence**.

Key insights

Study participants see the greatest need for innovation in four categories:

- Automation & efficiency
- Integration & harmonization
- User Experience & collaboration
- Data Analytics & AI

Focusing on these areas will help create a more sustainable, efficient, and value-added process for management.

Expectation towards auditors

Clients expect auditors to have industry experience, be efficient and collaborative, and to deliver high-quality results. Continuity in the audit team and a risk-based and entrepreneurial mindset are also highly valued.

Professionalism and expertise

- Clients expect auditors to have **strong technical and process expertise**, particularly in complex IT environments and industry-specific contexts.
- There is also a clear preference **for risk-based approaches** over template- or checklist-driven audits.

Consistency and continuity

- Clients value **continuity within the audit team** and prefer working with the same auditors over time to minimize repeated explanations and onboarding efforts.
- High auditor turnover or **frequent changes** in junior staff **are viewed as disruptive** and add to the workload for the audited organization.

Efficiency and pragmatism

- Clients expect efficient audits with **a solution-oriented approach** that focuses on relevant matters and avoids unnecessary bureaucracy.
- **Timely communication**, clear feedback, and strict **adherence to deadlines** are also highly valued.

Constructive collaboration

- Clients value auditors who engage in **open dialogue**, offer constructive feedback and **take the time to explain** findings and requirements.
- The also expect auditors to **understand the business context** and adapt their approach accordingly.

Quality and reliability

- Clients expect high-quality, reliable audit results accompanied by clear, **actionable recommendations.**
- They also value **clarity regarding the specific audit evidence required** for each control and the expected level of quality.

Outlook & recommendations

06

Outlook

As companies plan for the future of their ISAE/SOC reporting journey, the following market trends are expected to shape the evolution of ISAE/SOC reports:

Upcoming regulations

New regulations are emerging to address the evolving risks in technology, data governance and compliance. Organizations must implement **robust controls and ensure transparency to meet these requirements** and maintain stakeholder trust.

ESG & sustainability

ESG initiatives **require accurate reporting and accountability for sustainability-related data and processes**. Independent assurance of these metrics enhances credibility and boosts investor confidence.

Cyber Resilience Act

The Cyber Resilience Act (CRA) strengthens cybersecurity standards for products with digital elements, requiring manufacturers and retailers to ensure cybersecurity throughout the product lifecycle. **ISAE/SOC reports could help meet CRA customer requirements**.

AI Assurance

As AI systems become central to business operations, stakeholders expect fairness, transparency and reliability. **Demonstrating effective governance and control over AI models is essential to building trust**.

AI as enabler

AI is increasingly being used to automate critical processes, which amplifies operational and compliance risks. **Ensuring that AI-driven systems comply with control standards** helps mitigate errors and avoid regulatory breaches.

Recommendations for navigating the ISAE/SOC process

Wherever you are in your ISAE/SOC journey, these twelve actionable recommendations, drawn from the study and expert insights, offer valuable guidance. They highlight essential strategies to effectively navigate and manage current and future third-party assurance demands.

01 **Secure executive sponsorship,** as an ISAE/SOC report sends a strong signal to the market because it requires robust internal processes and committed leadership.

02 Establish **clear criteria that determine when an ISAE/SOC report is necessary** for a product and/or service. Involvement of the **Legal function** can support with providing clarity on the defined criteria and requirements.

03 Appoint a **dedicated individual to oversee the process**, ensuring adherence to deadlines and quality standards. Clear ownership, expectation management and **thorough documentation** will help mitigate the impact of staff turnover.

04 **Include commercial and marketing aspects** as part of your value proposition to end customers. ISAE/SOC reports have a cost, so it is natural that the burden is shared.

05 **Promote continuous improvement** by evaluating ISAE/SOC processes and control scope during each reporting period. Identify synergies across your assurance landscape (e.g., ISO 27001, BSI C5).

06 **Leverage GRC tools from the outset** to automate tasks such as planning, evidence collection and system description updates, helping to **reduce audit fatigue**.

07 **Select the appropriate report type** (e.g., ISAE 3402, ISAE 3000 or SOC2) to **align** with the services provided, **regulatory requirements** and/or **contractual agreements**.

08 **Begin with a minimal scope** and expand gradually as needed, ensuring the scope is confirmed with key customers. This approach allows time to institutionalize and **refine your processes**.

09 **Controls should support the overall Internal Control System**, compliance requirements and security posture. **Avoid relying on generic templates** and controls solely to meet standard requirements.

10 **Perform a readiness assessment** to verify that controls are properly designed and to **gather initial feedback on their auditability** and integration into operations.

11 **Prioritize the quality** of control execution and its documentation. Ensure the **appropriate evidence** is provided at the required standard and pre-align with your auditor to **avoid surprises**.

12 **Gather and share insights on leveraging Artificial Intelligence** in ISAE/SOC processes (e.g., updating control or system descriptions).

● Strategy / AI ● Process ● Scope / Quality

How can we help you

At KPMG, we bring extensive experience in ISAE/SOC reporting, having supported organizations for many years across diverse areas such as business operations, IT, cybersecurity, supply chain, and other specialized fields.

We assist organizations new to controls assurance with the design, implementation, and operation of effective assurance reviews. We do not believe in a one-size-fits-all approach; assurance reporting is a powerful tool for building trust, and the approach must be tailored to reflect each organization's unique services and risks.

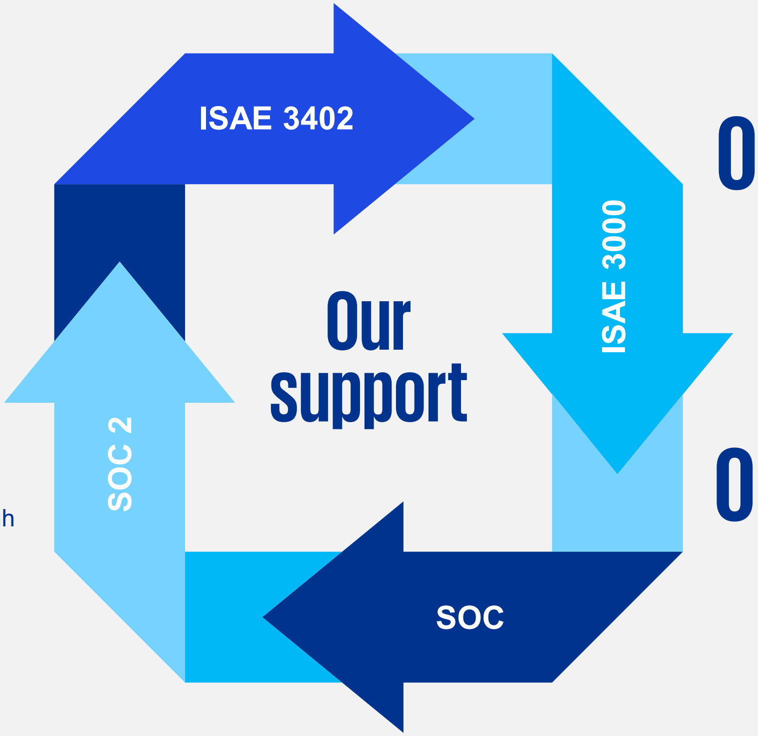
By partnering with our clients, we design customized assurance solutions that are efficient, effective, and aligned with their specific business and stakeholder needs.

Click here for more information on our services.

We can provide assurance using one or more of the available assurance standards and frameworks:

01 ISAE 3402

ISAE 3402 report for financial reporting purposes.



02 ISAE 3000

ISAE 3000 for a wide range of regulatory, operational or other subject matters (e.g., Cyber Resilience Act, ESG, AI).

03 SOC

SOC for cybersecurity report, based on TSP100 framework.

04 SOC 2

SOC 2 report (reported through the ISAE 3000 standard), based on the Trust Services Principles and Categories: security, availability, confidentiality, processing integrity and privacy.

If you are new to ISAE/SOC reporting, we can assist you in navigating through the regulatory landscape and in conducting a readiness assessment before starting a formal review cycle.

Your contacts

Stefan Wälti

Partner, Head of Assurance Technology
KPMG Switzerland
swaelti@kpmg.com

François El Assad

Director, Assurance Technology
KPMG Switzerland
felassad@kpmg.com

Alexander Cejka

Partner, Financial Services Technology
KPMG Switzerland
acejka@kpmg.com

Glossary

07

Glossary

DORA: The Digital Operational Resilience Act is an EU regulation focused on ensuring the digital resilience of the financial sector.

ESG: Environmental, Social and Governance refers to a framework that helps organizations integrate sustainability, ethical practices, and governance standards into their strategy and operations to address risks and create long-term value.

FINMA: The Financial Market Supervisory Authority is Switzerland's independent body for regulating financial markets.

GDPR: The General Data Protection Regulation is aimed at protecting the personal data of all individuals within the EU, regardless of where the organization is located.

ISAE: The International Standard on Assurance Engagements provide a global framework for assurance engagements that are not audits or reviews of historical financial information.

SEC: The Securities and Exchange Commission is a U.S. government agency responsible for regulating the securities industry, enforcing federal securities exchanges and other entities.

SOC Report: A System and Organization Control report is a third-party audit report that evaluates the internal controls of a service organization.

KPMG

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

kpmg.ch

Some or all of the services described herein may not be permissible for KPMG audited entities and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our Privacy Notice, which you can find on our homepage at www.kpmg.ch.

Create | CRT163108 | November 2025

Document Classification: KPMG Public