Shape the future with confidence

Are you ready for a smooth SOC 1 audit?

SOC 1 – System and Organization Controls for Financial Reporting.

The better the question.
The better the answer.
The better the world works.

Are you a SOC reporting newcomer?

Following the 7-steps-signpost could help you start your SOC 1 attestation journey.

Struggling with the answers?

Contact us for a non-binding SOC workshop.

Choose your individual service auditor

1 What report do I need?

SOC 1 Type 1 vs Type 2 report choice

2 Why do I want the report?

Scoping considerations - services, products, risk assessment, client requirements

3 Is my control framework prepared?

Control objectives - documentation, design, implementation, monitoring and testing

4 Are responsibilities clearly defined?

Mine, my clients' and subservice organizations'

5 When do I need the report?

Expectation of time horizon

6 Am I ready for the attestation?

Readiness assessment, timing

7 I am ready. What is next?

Attestation process, report delivery

1 What report do I need?

Why do I want the report?

SOC 1 reports are designed for service organizations that provide services that impact their clients' financial reporting. These reports assess the internal controls over financial reporting (ICFR) at the service organization.

SOC 1 reports are typically requested by the service organization's clients or their financial auditors to gain assurance regarding the effectiveness of controls related to financial reporting. There are two types of SOC 1 reports:

- **SOC 1 Type 1:** A SOC 1 Type 1 report evaluates the design and implementation of controls at a specific point in time.
- **SOC 1 Type 2:** A SOC 1 Type 2 report evaluates the design, implementation, and operating effectiveness of controls over a specified period (e.g., six or twelve months).

However, there is also the SOC 2 report which might be more suitable for your needs.

When to choose SOC 2 over SOC 1 attestation?

Choosing SOC 2 over SOC 1 can be beneficial if your organization provides „technical" services that focus on security, availability, processing integrity, confidentiality, or privacy of data, rather than directly impacting financial reporting. SOC 2 reports provide a broad assessment of your organization's controls related to these areas, which is often preferred by clients seeking assurance on data protection. SOC 2 compliance can also demonstrate your commitment to strong security practices, providing a competitive advantage and meeting industry-specific regulations or client expectations related to data security and privacy. For example, large data center providers typically issue SOC 2 reports for their clients.

Which type of SOC 1 report might be suitable for you?

The type of SOC 1 report you need depends on your specific requirements and the needs of your clients or stakeholders:

- A SOC 1 Type 1 report is useful if you want to provide assurance to your clients or stakeholders regarding the design of your controls. It is typically used to demonstrate the establishment of control objectives and the initial implementation of controls (i.e., it is issued in the first year of the audit).
- A SOC 1 Type 2 report is more commonly requested by clients or stakeholders as it provides a greater level of assurance about the ongoing effectiveness of your controls. It demonstrates that the controls have been implemented, operated, and monitored effectively over time. Typically, its coverage period is 12 months and it is issued annually.

Know the difference between types of SOC 1 report...

SOC 1 Type 1

Covers the controls and their suitability as of a specific date and provides a snapshot of the control environment at a particular point in time.

Focuses on the design of controls and provides an opinion on whether the controls are suitably designed to achieve the intended control objectives.

Evaluates the design of controls by reviewing the control descriptions, policies, and procedures. It does not include testing the operating effectiveness of controls.

Provides a lower level of assurance compared to a Type 2 report.

SOC 1 Type 2

Covers the controls and their suitability over a defined period, typically a minimum of six months and assesses the effectiveness of controls over time.

Goes beyond design and includes an assessment of the operating effectiveness of controls. It evaluates whether the controls were not only designed appropriately but also operated effectively throughout the specified period.

Evaluates both the design and operating effectiveness of controls. It includes testing the controls to ensure they were operating effectively throughout the assessment period.

Provides a higher level of assurance than Type 1 report and is typically required by your clients' auditors

2 What I want the report for?

What do you need for the first round of SOC 1 examination?

Your organization needs to have several key elements in place. These elements help you demonstrate the organization's control environment and ensure the effectiveness of its internal controls over financial reporting. It is important to note that the specific requirements for a SOC 1 examination may vary based on the organization's industry, the complexity of its systems, and the needs of its clients.

Scoping Considerations Checklist

- **Understand Client Requirements**
  Consider the requirements of your clients or business partners who are requesting the SOC 1 audit.
- **Identify Relevant Systems and Processes**
  Determine the services, products, areas, systems, processes, and controls that are in the scope of the audit.
- **Regulatory and Industry Standards**
  Take into account any regulatory or industry-specific standards that may influence the scoping of the audit.
- **Subservice Organizations**
  If your organization relies on subservice organizations that perform critical functions related to financial reporting (such as cloud service providers), evaluate their inclusion in the scope.
- **Risk Assessment**
  Conduct a risk assessment to identify the key risks associated with financial reporting.
- **Geographical Considerations**
  If your organization operates in multiple locations, determine the geographical scope of the examination.
- **Responsibilities**
  Consider the division of responsibilities for the service organization, subservice organization, and client.
- **Exclusions and Limitations**
  Identify any specific controls or areas that are explicitly excluded from the scope of the examination.

3 Is my control framework sufficiently mature?

Here are some of the essential requirements for a SOC 1 examination:

Control objectives

Defined Control Objectives

The company needs to establish clear control objectives related to financial reporting. The control objective is a specific goal that aims to ensure the effectiveness and reliability of organization's internal controls over financial reporting.These control objectives should align with the organization's processes and the needs of its clients who rely on the company's services for their financial reporting requirements.

Documented Control Activities

The company must have documented control activities that demonstrate how it achieves the defined control objectives. This includes documented policies, procedures, process flows, and other relevant documentation that outline the controls in place.

Control Design and Implementation

The controls should be appropriately designed and implemented to address the defined control objectives. They should be designed to mitigate risks and ensure the accuracy, integrity, and completeness of financial reporting.

Regularly Updated Control Framework

The company needs to have processes in place for regular updates of its control framework. This demonstrates the ongoing commitment to maintain and improve internal controls over financial reporting to meet changing business or regulatory needs and evolving risks.

Documentation and Evidence

The company should maintain adequate documentation and evidence to support the design, implementation, and operating effectiveness of its controls. This includes control descriptions, policies, procedures, testing results, and other relevant documentation.

Risk assessment

Risk Assessment and Mitigation

The company should conduct regular risk assessments to identify and assess potential risks that could impact financial reporting. It should have measures in place to mitigate these risks and ensure the reliability of financial information.

4 Are responsibilities clearly defined?

How are responsibilities divided?

In a SOC 1 examination, there are distinct responsibilities for the service organization, subservice organization, and client. It is essential for all parties involved to understand their respective responsibilities and work collaboratively to ensure the effectiveness of internal controls and the overall success of the SOC 1 examination process.

Usually, the main responsibility lies with service organization which has defined Control Objectives, Controls within these objectives and responsible stakeholders (Control Owners) for each control. However, there are cases when the responsibility is rather on the client's side (Complementary User Entity Controls) or subservice organization (Complementary Subservice Organizations Controls):

Product (in-scope services)

Control Framework

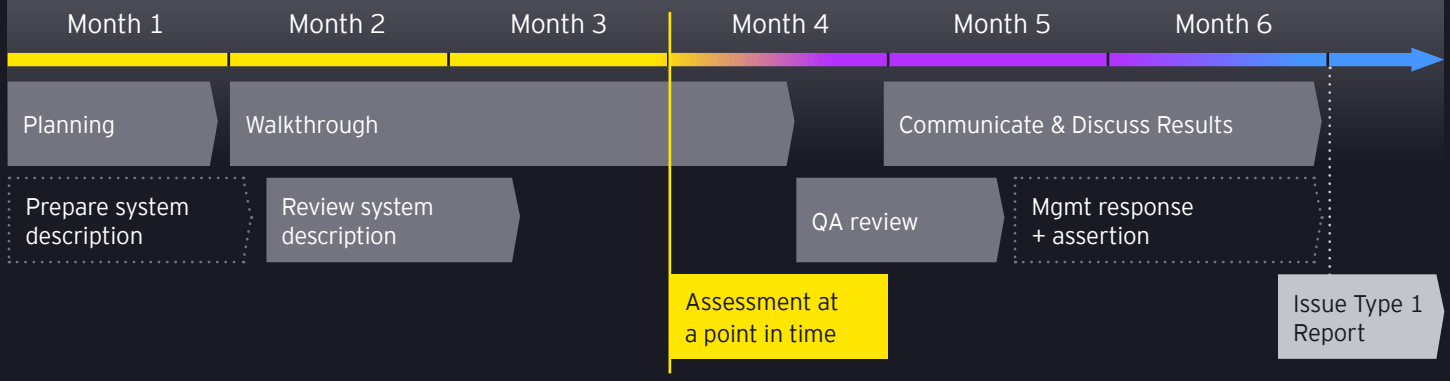
Subservice organization	You (Service organization)	Your client
Complementary Subservice Organizations Controls	Control Objectives	Complementary User Entity Controls
(controls where your supplier is responsible for their execution)	Controls	(controls where your client is responsible for their execution)
	Control Owners	

5 When do I need the report?

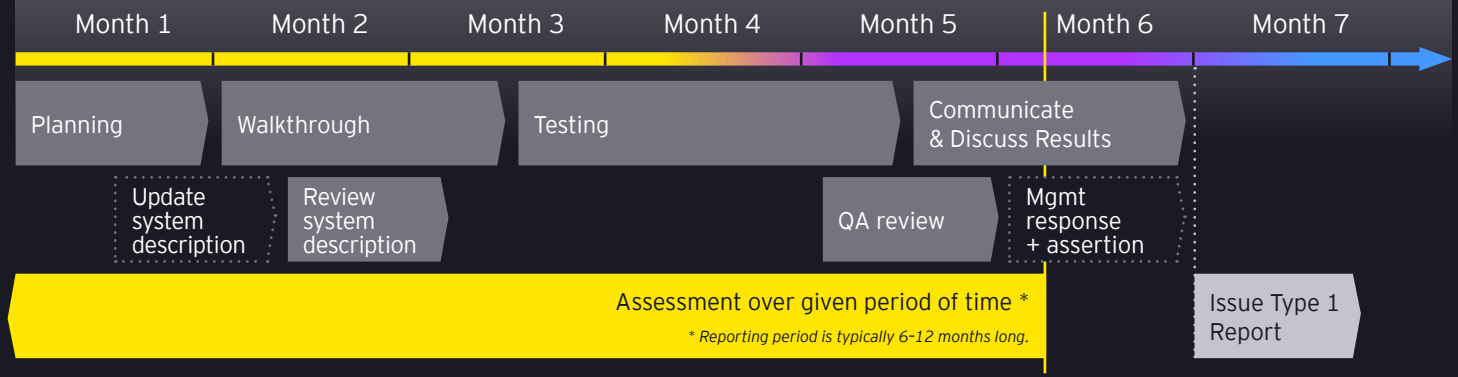
What is the expectation of time complexity?

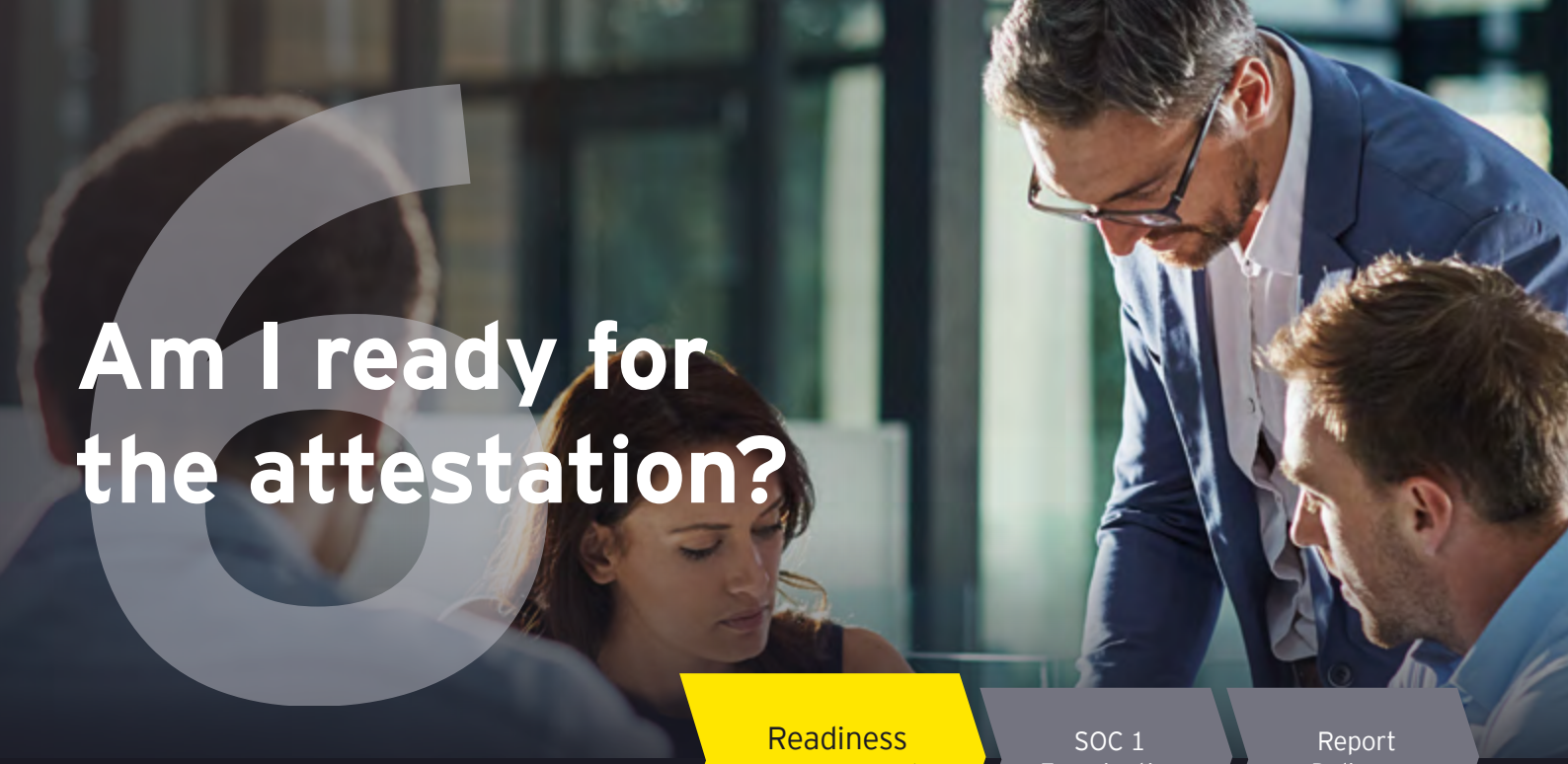
Timeline depends on whether a SOC 1 Type 1 report or a SOC 1 Type 2 report is chosen.
The following timelines might help to better understand timing needed for each type of attestation.

Type 1 reporting timeline



Type 2 reporting timeline





Am I ready for the attestation?

Readiness assessment | SOC 1 Examination | Report Delivery

Do you know your company's environment well?

A readiness assessment, in the context of SOC reporting, is a process that helps evaluate an organization's preparedness for undergoing a SOC examination. It involves assessing the organization's controls, processes, and documentation to determine if they meet the requirements of the chosen SOC report.

What are the benefits of readiness assessment?

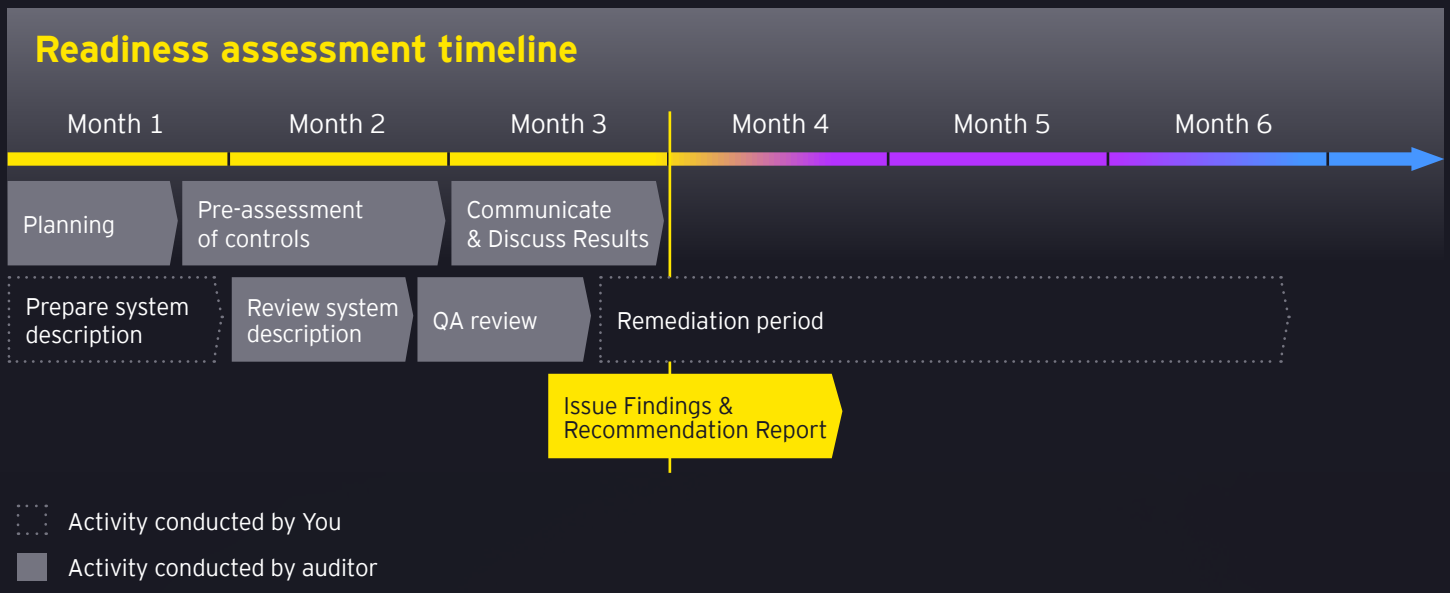
A readiness assessment is a proactive approach to ensure your organization is well-prepared for the SOC examination. It helps identify and address control deficiencies, improve processes, and provide assurance to clients and stakeholders about the effectiveness of your controls. By conducting a readiness assessment, you can increase the likelihood of a successful SOC examination and instill confidence in your organization's control environment.

Here's why a readiness assessment is important and why you may need it:

- Evaluate Control Effectiveness
- Identivy Control Deficiencies
- Assess Documentation and Evidence
- Mitigate Risk and Enhance Compliance
- Gain Stakeholder Confidence
- Improve Efficiency and Timeliness
- Faciliate Communication and Colaboration

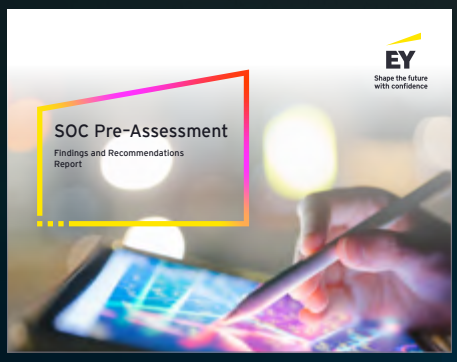
What about the timeline needed for Readiness assessment?

It's important to consider that a readiness assessment before the SOC examination may significantly contribute to a successful and timely issuance of the final SOC report. This additional time allows for a thorough evaluation of your company's environment, including controls, processes, and documentation, ensuring they meet the requirements of the chosen SOC report.



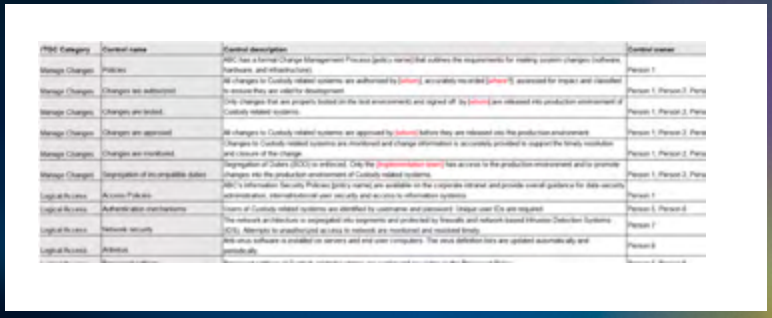
What are typical outputs of SOC pre-assessment?

Findings and Recommendations report

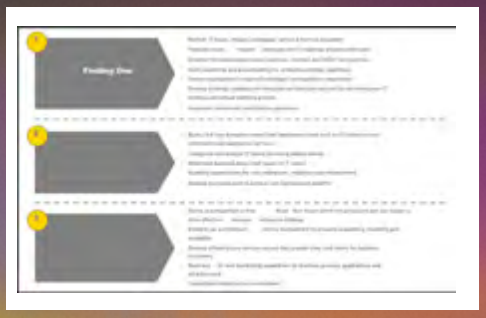


Guidance on Control Framework definition

Guidance on Draft system description / narratives



Prioritized roadmap



7

I am ready. What is next?

Readiness assessment | **SOC 1 Examination** | Report Delivery

What are the steps of SOC 1 examination?

The examination follows a systematic process to evaluate the effectiveness of a service organization's internal controls over financial reporting. Here's an overview of the typical steps involved in conducting a SOC 1 examination:

Scoping and Planning

- The examination begins with scoping and planning activities, taking into account scoping considerations, considering the readiness of the control framework, available resources, and capacities. The examination period is determined, which can be either a specific date (for SOC 1 Type 1) or a specified period (for SOC 1 Type 2).
- Based on that, the organization and service auditor should develop an audit plan. This audit plan outlines procedures, methodologies and timelines for the examination,ensuring that they are aligned with the organization's readiness and available resources.

Control Evaluation

- The service auditor assesses the design and implementation of the service organization's controls. This involves reviewing control documentation, policies, procedures, and other relevant documentation. The service auditor evaluates whether the controls are designed appropriately to achieve the defined control objectives and if they have been implemented effectively.

In a SOC 1 report, there is a distinction between IT general controls (ITGCs) and business controls:

IT General Controls

They focus on the overall IT infrastructure and environment.

Examples of ITGCs include access controls, change management processes, backup and recovery procedures, network security, and system monitoring.

ITGCs are important for all areas of an organization's financial reporting.

Business Controls

They are also known as application controls or business process controls, are specific controls embedded within business processes and applications.

These controls directly impact financial reporting.

Examples of business controls include segregation of duties, approval workflows, data validation, reconciliation processes, and transaction monitoring.

Control Testing

- The next step is to test the operating effectiveness of the controls. The service auditor selects a sample of controls and performs testing procedures to assess whether the controls are operating as intended. This typically involves examining evidence, conducting interviews with relevant personnel, and performing walkthroughs of key processes.

Audit Evidence Documentation

- Throughout the examination, the service auditor documents the procedures performed, the evidence obtained, and the results of the testing. This documentation provides support for the conclusions reached and forms the basis of the final SOC 1 report.

Reporting

- Once the examination is complete, the service auditor prepares the SOC 1 report. The report includes a description of the service organization's controls, the control objectives, and the results of the examination.
- For a SOC 1 Type 1 report, the report focuses on the suitability of the design of the controls. For a SOC 1 Type 2 report, the report evaluates both the design and operating effectiveness of the controls over the specified period.

Issuance of Report

- The final SOC 1 report is issued by the service auditor to the service organization. The report is typically provided to the service organization's management, clients, and other stakeholders who have a need for the information to evaluate the effectiveness of the organization's controls over financial reporting.

Contact us for a non-binding SOC workshop.

What does the SOC 1 report contain?

The SOC 1 report consists of several sections that provide information about the service organization's controls and the results of the examination. The content of the report may vary depending on whether it is a SOC 1 Type 1 or Type 2 report. Key sections typically include:

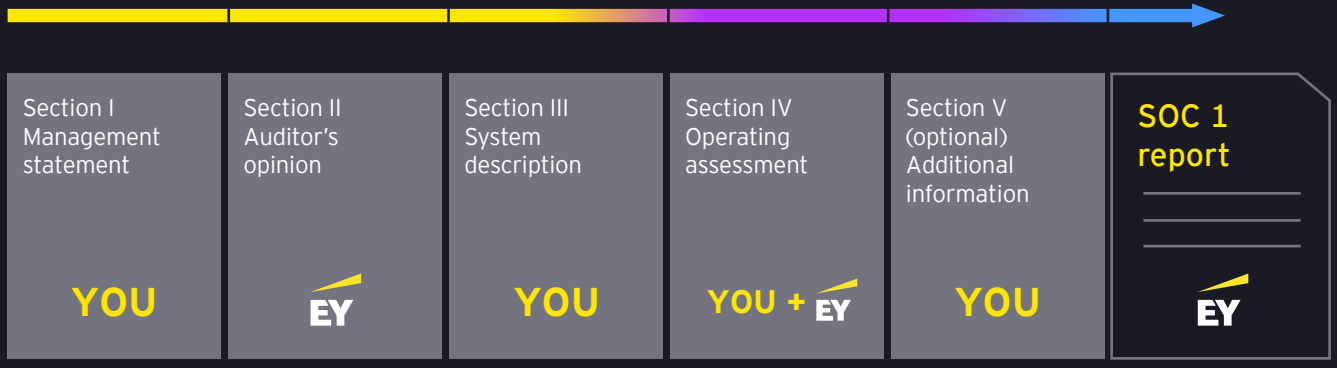
a. Service Auditor's Opinion: This section contains the opinion of the CPA firm regarding the fairness of the presentation of the service organization's controls in achieving the control objectives.

b. Service Organization's Description of Controls: This section describes the service organization's control environment, including control objectives, systems, processes, and relevant control activities. It provides a detailed overview of the controls in place to support financial reporting.

c. Tests of Controls and Results: This section outlines the testing procedures performed by the CPA firm to assess the operating effectiveness of the controls. It presents the results of the testing, including any identified control deficiencies or exceptions.

d. Other Information: The report may include additional information deemed relevant, such as a summary of the CPA firm's methodology, the period covered by the examination, and any limitations on the scope of the examination.

SOC 1 Report Structure and Responsibilities



What do you need to consider during the SOC 1 report delivery?

Restricted Distribution

SOC 1 reports are typically restricted in their distribution. They are intended for specific parties, such as the service organization's management, clients, and other authorized stakeholders. The distribution of the report is determined based on agreements between the service organization and the users of the report.

Electronic or Physical Delivery

The SOC 1 report can be delivered in either electronic or physical form, depending on the preferences of the service organization and the users of the report. Electronic delivery is common and may involve sharing the report securely through a file-sharing platform or sending encrypted copies via email. Physical delivery involves printing and mailing physical copies of the report to the intended recipients.

Use of the Report

Once the SOC 1 report is delivered, the service organization can provide it to its clients and other stakeholders, as necessary. The report is often used by clients to evaluate the effectiveness of the service organization's controls over financial reporting and to support their own compliance and auditing requirements.

Public information

It is recommended that you provide information regarding the existence of your SOC1 report on your website. Sharing this information can enhance your competitiveness in the market.

Contact us for a non-binding SOC workshop.

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

ey.cz

Let's start the conversation.

Josef Duben
Senior Manager
+420 731 642 752
josef.duben@cz.ey.com

Jan Chleborád
Manager
+420 704 865 133
jan.chleborad@cz.ey.com

Contact us for a non-binding SOC workshop.