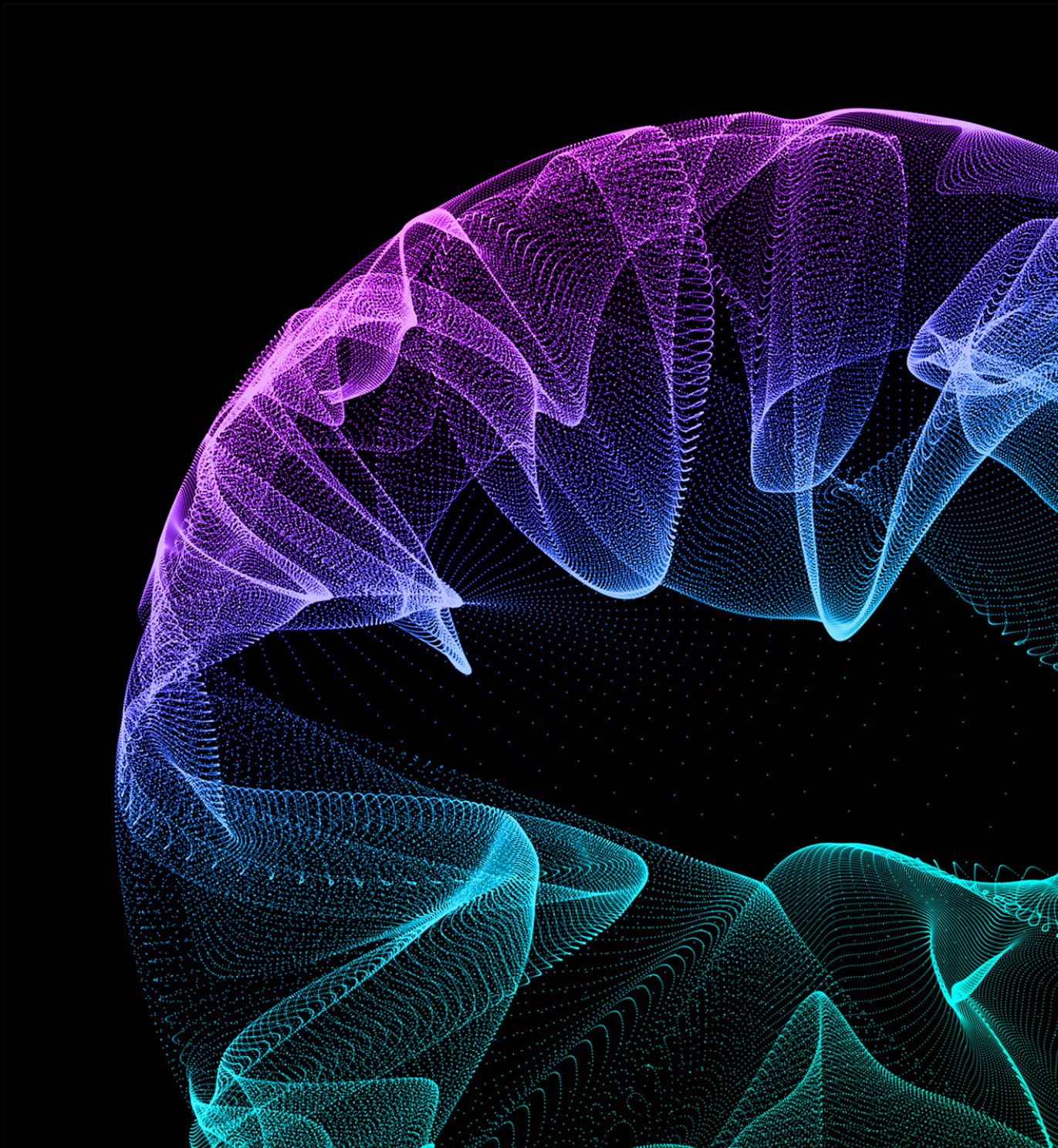
Deloitte.

Control IT
Reviewing third-party SOC reports



Introduction

In today's rapidly evolving technological landscape, the importance of robust IT risk management and control mechanisms cannot be overstated, especially for organizations and their auditors striving for Sarbanes-Oxley (SOX) compliance. Deloitte's Control IT Thoughtware Series delves into critical IT risk and control topics to explore emerging trends and case studies and to offer practical, insightful leading practices and guidance tailored to the needs of professionals in the IT risk and compliance realm. We look forward to helping your organization manage these risks effectively and emerge stronger and more resilient in the face of uncertainty.

What to focus on in a SOC review

To meet Sarbanes-Oxley requirements, companies assess and monitor the outsourced service third-party providers that are relevant to their financial statements. A System and Organization Controls (SOC) report is a third-party audit report that provides detailed information about the controls and processes at the service organization. These reports are issued by independent auditors and are designed to provide assurance to stakeholders, user entities (such as customers, partners, and regulators), and external auditors of user entities about the effectiveness of the service organization's controls.

Reviewing SOC reports is a critical component of third-party risk management strategy to monitor third-party control environments. As enterprises expand their engagement with third parties, obtaining and reviewing SOC reports is becoming more critical. Auditors are required to perform and document more thorough reviews and analysis of the SOC reports and are pushing back on user entities to take a deeper look at SOC reports as part of their compliance and SOX programs.

Control IT - Reviewing third-party SOC reports

When user entities perform SOC reviews, it is critical to ask and document your answers to the following key questions:

System description: Are the boundaries of the system description clear, including which operations are covered by the description and controls and are relevant to my organization?

Scope coverage: Does the report cover all services, systems, locations, SOC1 control objectives and/or SOC2 Trust Services Criteria (TSC) and controls that are relevant; and is it easy to understand and decipher?

Period: Is the coverage period optimal? Are there additional actions my organization should take for gaps in report coverage? If so, what are those?

Credentials: Is the auditor qualified and reputable?

Opinion and exceptions: Is the report opinion qualified, and what is my impact? Are there testing exceptions, and were acceptable responses/exposure checks provided by the service organization? Was remediation tested by the service auditor?

Complementary user entity controls (CUECs): Are all CUECs identified in the SOC report? Are they considered relevant and implemented and documented at my organization?

Subservice organizations: Are subservice organizations identified as relevant, and is it necessary to obtain those additional SOC reports?

In this series, we will help you, as a user entity, enhance your assessments and modernize your reviews of SOC reports. To make your review of service organization SOC reports more meaningful and effective, we will tackle each of these questions in the next sections with suggested leading practices and pitfalls to avoid.

Practical & insightful guidance

1: Understanding the service organization

The System Description section of the SOC report is a critical component that provides essential information for understanding the scope, control environment, risk management, compliance, and security posture of the service organization. Reviewing this section thoroughly enables user entities to make informed decisions, manage risks effectively, and understand how the scope relates to their organization.

Leading practices: User entities should understand the relationship with a relevant service organization and determine whether the SOC report has the required coverage for the services provided. User entities should review the boundaries of the SOC report and confirm the following:

- Services provided to your user entity and relevant locations are covered by the SOC report.
- System components (infrastructure, software, tools, and data) are included within the scope.
- Relevant business and IT processes (as applicable) and controls are included.
- Report covers the applicable legal, regulatory, and industry standards the user entities are using the report for.
- Relevant key outputs, such as reports or files, provided or made available to your user entity, are identified in the description of the system and tested within the report.

If you have questions on the SOC report coverage, it is recommended to reach out the service organization to ask clarifying questions and consider making recommendations to them to improve their report content.

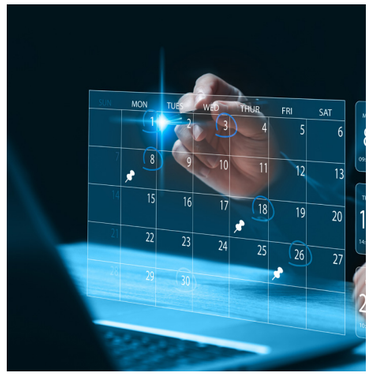
Learn about the pitfalls:

User entities may fail to fully understand the scope, findings, and implications of the report due to complex technical jargon or unfamiliar terminology resulting in failure to identify which services are used. This can lead to the wrong report being obtained and relied upon. Additionally, the whole report may be inappropriately determined to be relevant when some of those services may not be applicable to the user organization.

Control IT - Reviewing third-party SOC reports

2: Report period

User entities should understand if the SOC examination period aligns with your organization's fiscal year or intended reliance period to determine whether the report provides acceptable coverage. The length of the period not covered by the service auditor's report is called the "bridge period." A long bridge period can lead to increased risks and reduced assurance. If a significant time period has elapsed, the user entity (often pressured by the needs of its auditors) may need to perform additional procedures such as engaging with service providers to conduct additional assessments, enhancing monitoring controls, and updating risk management practices.



Leading practices: User entities should request bridge letters, which are letters from the service organization that indicate whether there has been material changes in the service organization's controls since the time period covered by a service auditor's report. To address lengthy bridge periods, organizations should consider the following additional procedures to gain more assurance near the end of the bridge period, including:

- Enhanced monitoring of the service organization in the bridge period.
- Contacting the service organization to obtain specific additional information.
- Requesting that a service organization have its service auditor perform procedures that will provide sufficient evidence.
- Obtaining evidence that controls continue to operate effectively closer to the as-of date.

Consider using your influence over the service organization to request changes to the SOC audit coverage period to plan for timely future SOC reports. If your user entity does not have influence over certain service organizations regarding SOC audit coverage and performing additional procedures, you should consider scope limitation as mentioned in the Pitfalls section.

Learn about the pitfalls:

User entities need to consider whether an issue or deficiency exists when the bridge period is long and the user entity has not taken steps to gain additional assurance over the operating effectiveness of the controls and does not have robust user entity monitoring controls. Not considering the inappropriate period coverage for the financial statements audit, which may result in deficiency, and evaluating for significance could have an impact on SOX compliance.

Additionally, not having a right-to-audit contract clause with the ability to independently evaluate whether service organizations are meeting their obligations and maintaining effective controls may limit user entities' ability to perform additional procedures onsite at service organizations.

3: Relevant controls

Reviewing the controls in Section 4 of a SOC report is a critical part of understanding the effectiveness of the service organization's control environment. Section 4 includes detailed descriptions of the control objectives and the specific controls in place to meet those objectives as well as testing procedures, results, and management's responses to testing exceptions that could also be included in Section 5, the unaudited section.

Leading practices: User entities should evaluate the relevant risks in their environment and map control objectives and controls from the report to address those risks. User entities should evaluate the efficacy of the testing procedures and results including:

- Review the list of control objectives to understand what the service organization aims to achieve.
- Evaluate whether the design of each control is adequate to meet the control objectives.
- Ensure that the controls are consistently applied across the relevant areas (relevant IT areas and business processes).
- Review the testing performed by the auditor to ensure that the controls have been implemented as described.
- Assess whether controls follow AICPA guidance and/or are meeting the user entities' needs and framework requirements (such as SOX, COBIT, NIST, ISO, etc.).

Reach out to the service organization for clarification on any unclear points or to obtain additional information.

Learn about the pitfalls:
Without a thorough review, the user entity may not fully understand the service organization's control environment, including the specific controls in place and how they operate. Regulatory requirements often mandate specific controls and processes. Without a thorough review, the user entity may overlook critical compliance-related controls.

4: Complementary user entity controls (CUECs)

CUECs are controls that the user entity is responsible for implementing to complement the controls of the service organization. These controls are listed in the report, but are not tested. They can be essential for achieving the control objectives because the service organization's controls alone may not be sufficient without the user entity's complementary controls.

Leading practices: Relevant CUECs should be identified, mapped, and evaluated to understand the purpose and function of each CUEC to achieve your objectives. User entities should:

- Determine which CUECs are relevant and applicable to your organization based on services utilized.
- Ensure that the relevant CUECs are implemented within your organization.
- Integrate CUECs with your internal control framework to ensure a cohesive control environment.
- Periodically test the effectiveness of the implemented CUECs.
- Evaluate deficiencies in CUECs in conjunction with exceptions in related SOC control objectives.

We recommend user entities create a matrix of all CUECs and document rationale around relevance.

Learn about the pitfalls:
User entities might omit evaluation of a relevant CUEC identified in the report, which is required to meet the control objective they are relying upon. There may be other CUECs not suggested by the SOC report, so consider other tailored CUECs at your organization.

5: Exceptions

Reviewing exceptions in SOC reports is a critical task to ensure the service organization's control environment is effective and that any report qualification and testing exceptions are properly understood and addressed. Exceptions identified in the SOC report should be evaluated by the user entities to determine if there is an impact on your risk assessment, internal controls, and/or assurance requirements (SOX).

Leading practices: User entities should review and evaluate the exceptions for relevant controls. They should consider documenting why an exception is or is not considered relevant and consider the following:

- Enhanced monitoring of the service Understand the nature of the testing exceptions identified and relevance of control.
- Determine which control objectives are impacted, whether the exception leads to a qualified opinion, and whether the qualified opinion affects control objective(s) relevant to your user entity.
- Assess the severity and evaluate the risk associated with the exception (process improvement or deficiency or significant deficiency). Consider the potential impact on the service organization's operations and on your user entity.
- Determine whether alternate controls exist within the report to mitigate the risk exposed by the exception.
- Review procedures the service organization and/or auditor may have performed to assess whether the risk was exposed.

We recommend user entities create a matrix of testing exceptions and document your conclusions. If necessary, communicate with the service organization's management and auditors to gain further insights into the exceptions.

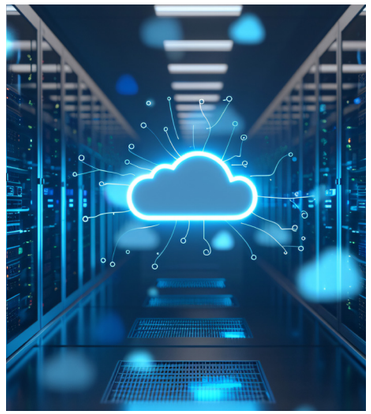
Learn about the pitfalls:
Lack of in-depth review and response to exceptions in the Service Auditor Report could result in overlooked risks, inaccuracies, and deficiencies that go unevaluated for your SOX requirements. Important details about control gaps or deficiencies may be missed if Section 4 is not reviewed carefully.

6: Subservice organizations

User entities should evaluate carved-out subservice organizations to determine whether their processing and IT activities affect your organization. Example entities include cloud service providers, data center hosting, customer service support, etc. Obtaining a comprehensive view of the entire service delivery and reviewing subservice vendors in a SOC report is crucial for risk management since subservice vendors could affect the overall control environment. If there are relevant subservice organizations identified within the SOC report for the subservice organization, the user entity should obtain additional SOC reports for such subservice organizations.

Learn about the pitfalls:
Without assessing subservice organizations, the user entity may have an incomplete understanding of the risks associated with the service being provided, and important control gaps or deficiencies at the subservice organization level may be missed. Without understanding the controls and risks associated with subservice organizations, user entities may be ill-prepared to respond to incidents that originate from or involve these organizations.

Leading practices: For relevant subservice organizations, you should obtain additional SOC reports for evaluation. User entities should leverage the complementary subservice organization controls (CSOCs) to help guide them to which parts of the subservice organization's SOC report would be considered relevant to them. User entities should review prior-year reports to appropriately plan for the upcoming year. If a SOC report is not available for the relevant subservice organization, user entities should plan for additional/alternative procedures.



Control IT - Reviewing third-party SOC reports

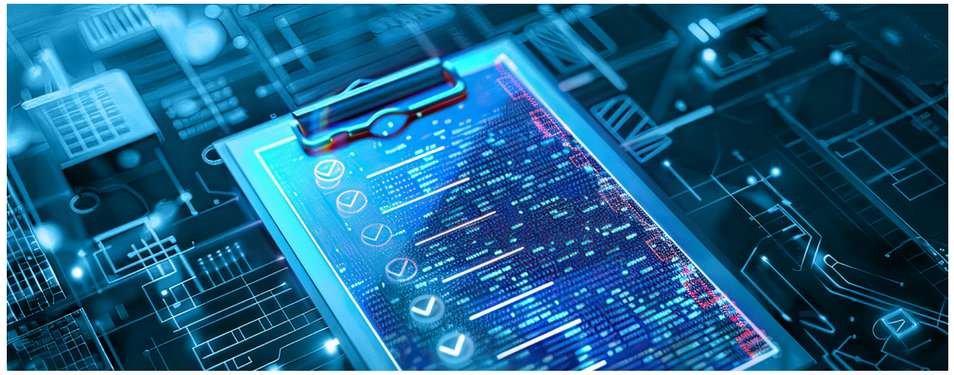
Modernization

Getting the fundamentals right around performing SOC reviews is critical to maintain a robust third-party risk management strategy. In addition to the leading practices outlined above, Generative AI (artificial intelligence) can be a valuable tool in the review process of SOC reports by assisting with various tasks such as summarization, anomaly detection, and compliance checks. Sophisticated user entities at the forefront of AI adoption are creating efficiencies with these tools by:

- Generating concise summaries of long SOC reports; highlighting key findings, control deficiencies, and areas of improvement; and breaking down complex sections into more digestible snapshots.
- Identifying unusual patterns or anomalies in the data presented in SOC reports that requires further investigation.
- Assisting in cataloguing the controls described in the SOC report to relevant compliance frameworks (e.g., ISO, NIST), ensuring that necessary controls are in place.

However, it is critical to understand the capabilities and limitations of AI in this context. Choose AI tools that are specifically designed for document analysis and compliance checks. Ensure they have robust security measures and AI risk management in place. By carefully implementing and integrating AI tools, user entities can streamline their SOC report review processes.

Deloitte is available to help you develop your third-party risk management programs, enhance your SOC evaluation controls, train your risk management teams, and advise on SOC reporting requirements and exceptions.



Contacts

Sara Lademan
IT & Specialist Assurance Leader
Advisory Partner
Deloitte & Touche LLP

Tel: +1 312 486 2981
Email: slademan@deloitte.com

Authors

Todd E. Morgenthaler
Advisory Managing Director
IT&SA US COMM A&T
Deloitte & Touche LLP

Tel: +1 312 486 2017
Email: tmorgenthaler@deloitte.com

Sarika Singh
Advisory Senior Manager
IT&SA US COMM A&T
Deloitte & Touche LLP

Tel: +1 612 298 5271
Email: sarsingh@deloitte.com

Deloitte.

MAKING AN IMPACT THAT MATTERS since 1845