



Deloitte.

A practical guide to SOC readiness

OCTOBER 2026



Table of contents

1	Introduction	3
2	The potential value of readiness in SOC examinations	4
3	A readiness pathway	5
4	Common SOC readiness pitfalls—and ways to reduce them	8
5	Leading practices for SOC examination readiness	10
6	Deloitte's Third-Party Assurance (TPA) Readiness SelfAssess™ tool	13
7	Industry-leading advice for SOC readiness	14
8	Get in touch	15



Introduction

System and Organization Controls (SOC) standards, developed by the American Institute of Certified Public Accountants (AICPA), offer a consistent, independent framework for evaluating the design and operation of controls at service organizations. These standards focus on controls that may affect financial reporting (SOC 1) and trust services criteria (TSC) such as security and availability (SOC 2).

The resulting examinations, called SOC reports, present an independent attestation related to controls relevant to SOC 1 and SOC 2. They can allow service organizations to address Sarbanes-Oxley Act (SOX) needs for user entities, reduce repetitive documentation requests, and help address customer, regulatory, contracting, and broader risk management expectations.

Whether your organization is new to SOC reporting or looking to expand the existing types of reports obtained about products and services, a common question is: Where do we start?

A readiness assessment is a practical starting point. Conducted before attestation, it allows organizations to evaluate whether controls are appropriately designed to meet applicable SOC requirements, analyze gaps, and prioritize remediation efforts. Typical readiness outcomes may include defining the SOC scope, documenting the current state of controls, outlining complementary user entity controls (CUECs), and drafting the initial system description and remediation plan.

The sections ahead offer actionable guidance for preparing for a SOC engagement. Read on to explore a readiness pathway, common pitfalls, and leading practices that may make the SOC examination process smoother.



01

02

03

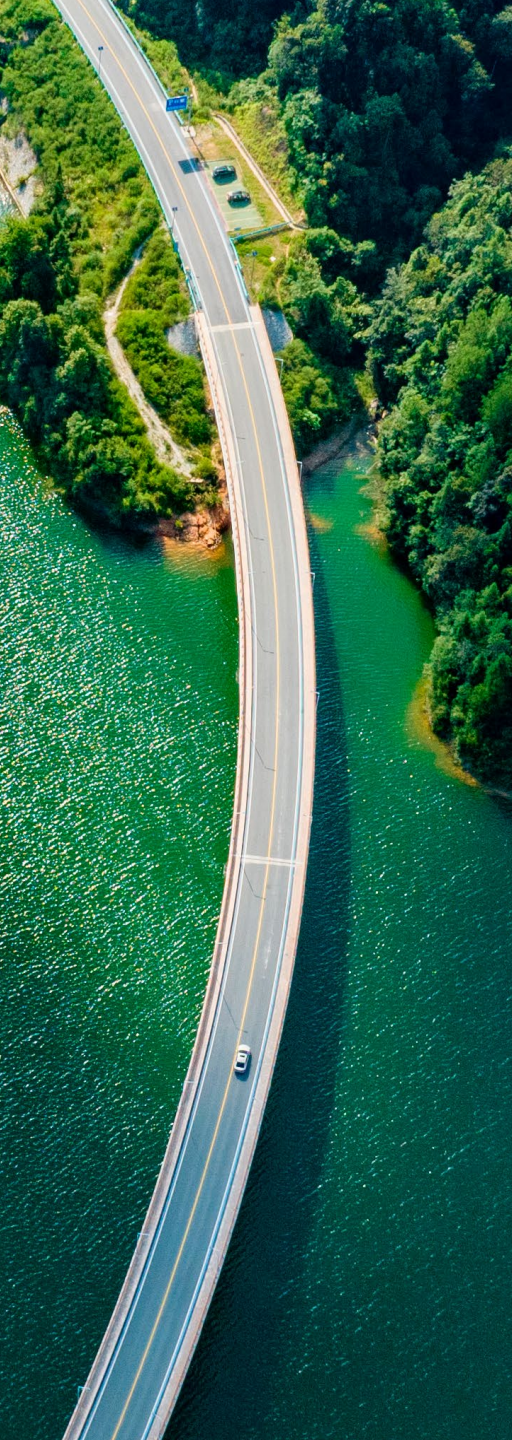
04

05

06

07

08



The potential value of readiness in SOC examinations

SOC examinations typically benefit from careful preparation. Organizations can use readiness to test whether controls are appropriately designed, supported by evidence, and aligned to the applicable SOC framework. Readiness can allow teams to surface weaknesses in control design, documentation, and operations early in the process. This allows for more time to remediate and document changes ahead of the examination, reducing the risk of surprises during fieldwork and helping to create a more efficient examination process.

Beyond examination mechanics, readiness could help build stakeholder confidence by signaling a mature and proactive approach to risk and compliance management. This can lead to increased customer trust and stronger relationships with clients. In that way, readiness efforts can help shift from operations to strategy, supporting business growth and allowing organizations to position themselves to meet requirements for larger clients.

Readiness assessments can also provide the opportunity to evaluate and refine the scope of a SOC examination before entering the attestation period. This includes considerations such as which products, services, systems, locations, processes, and control domains should be in scope, as well as whether a SOC 1 or SOC 2 examination is better aligned with the organization's objectives and customer expectations. Organizations can also assess whether they are better positioned to begin with a more narrowly tailored scope that can effectively meet stakeholder needs.

Furthermore, these assessments can allow the organization to translate identified gaps into actionable findings and remediation plans, with defined owners, sequencing, and target dates mapped back to a future SOC attestation report. As part of the assessment, organizations can evaluate the severity and nature of control deficiencies, determine root causes, and define practical corrective actions before the examination begins. Through the organization's development of a remediation roadmap, including defined test steps and evidence expectations, stakeholders can envision where the organization could be once the process is complete.



01

02

03

04

05

06

07

08

A readiness pathway

A SOC readiness assessment can reduce the risk of findings during an examination by identifying control gaps early and allowing opportunity for remediation before the SOC examination. This can allow your organization to enter the examination process with greater confidence and to potentially come away with fewer surprises.

A readiness assessment may include the following steps:

- **Consider the timeline from readiness to attestation:** Start by establishing a realistic plan from the readiness assessment through the start of the SOC examination. This typically includes time for gap identification, remediation, control maturation, evidence collection, and management review so the organization can begin the attestation process with sufficient preparation. In practice, organizations are generally better positioned to move into attestation within 12 months of the readiness assessment; if more time passes—or if there are significant changes to the system, scope, or control environment—the readiness results may need to be revisited or refreshed. When it comes to scheduling, it's worth noting these differences between type 1 and type 2 reports:
 - A type 1 report can usually be completed relatively quickly once controls are designed and implemented, since it provides a point-in-time view of the control environment.
 - A type 2 report takes longer because controls should operate for a defined period to demonstrate operating effectiveness—often at least six months for SOC 1, and commonly three to 12 months for SOC 2, with six months as a leading-practice target.



01

02

03

04

05

06

07

08



A readiness pathway (cont.)

- **Identify and align stakeholders:** A SOC readiness assessment often originates with a customer or client request. With an understanding of the client need, determine the specific individuals and teams that should take part in the readiness effort, such as control owners, process stakeholders, IT, security, compliance, legal, and executive sponsors. Early alignment helps clarify roles, responsibilities, and decision-making authority throughout the assessment and remediation process.
- **Scope the examination:** Define the boundaries by identifying the systems, products, services, locations, processes, and TSC (SOC 2) or control objectives (SOC 1) that might be included. Scoping should also consider the intended report users, relevant subservice organizations, select technologies, and exclusions or limitations that may affect the examination approach. Scoping efforts help focus the readiness process on the areas relevant to the report and reduce the risk of gaps, inefficiencies, or misalignment during attestation.
- **Map data flows and control processes:** Document how relevant data, transactions, and system activities move through the control environment, including certain handoffs, supporting technologies, and points of control execution. This helps establish the completeness of scope and provides context for evaluating risk and control coverage.
- **Conduct interviews to analyze the current state of controls:** Meet with control owners to understand how controls are designed and implemented in practice. These interviews and reviews of available documentation help analyze whether controls are formally defined, consistently executed, and supported by documentation and evidence aligned to the relevant SOC 1 control objectives or the service commitments and system requirements tied to the SOC 2 TSC.



01

02

03

04

05

06

07

08

A readiness pathway (cont.)

- **Identify gaps in meeting the control objectives or TSC:** Analyze areas where controls may be missing, insufficiently designed, inconsistently performed, or poorly documented and therefore do not fully meet the stated control objectives or TSC. It's important to address gaps before the examination begins. This gap assessment can help management understand where additional effort may be needed before attestation. Under the AICPA attestation standards, control deficiencies identified during testing are expected to be reflected in the report, as well as nonoccurrence of control activities in which a control did not work and a conclusion, therefore, could not be reached.
- **Remediate gaps and strengthen documentation:** Management is responsible for addressing identified gaps and overseeing remediation efforts. Remediation may include designing and implementing new controls, enhancing the consistency of existing controls, clarifying roles and procedures, and enhancing documentation and evidence to provide guidance on operating effectiveness.
- **Draft an initial system description:** Management is responsible for preparing an initial system description that clearly explains the services and system components in scope, the applicable control objectives or TSC, and the control activities intended to address them. The description should define system boundaries and summarize relevant aspects of the environment, such as infrastructure, software, people, processes, and data. It should also address specific service commitments, system requirements, and CUECs or complementary subservice organization controls (CSOCs), so roles and responsibilities are clearly understood. Developing this draft during readiness can help management validate scope, align control documentation, and analyze areas that may need refinement before the SOC examination begins.





Common SOC readiness pitfalls—and ways to reduce them

SOC readiness efforts usually don't break down because of one major control failure. More often, challenges arise from a series of planning, coordination, scoping, and documentation issues that become more difficult to manage once the examination is underway. An effective way to reduce the likelihood of these pitfalls is to approach readiness like a structured program—with clear ownership, defined timelines, and well-established evidence expectations—rather than a last-minute compliance exercise. Below are common pitfalls and the practical moves that can help you proactively reduce the likelihood they occur.

- **Lack of a clear readiness plan:** Without an in-depth and defined readiness plan, certain activities may be missed, timelines can slip, and risk can increase. To reduce these issues, align early with your SOC adviser on a plan that covers scoping, control design, evidence collection, remediation, and a final attestation readiness check before the examination begins.
- **Poor scoping:** If systems, products, services, locations, processes, and TSC or control objectives aren't clearly defined during scoping exercises, rework and engagement delays often follow. Reduce this by documenting scope early in plain language; test it with business, IT, and compliance stakeholders; and align it to the system description and applicable criteria before readiness begins.
- **Starting late:** When readiness begins too close to the desired report date—especially where client or contractual commitments are involved—there may not be enough time to remediate deficiencies and demonstrate consistent control operation. One way to reduce this is to work backward from the desired report date and begin the examination period only after critical gaps have been addressed.



01

02

03

04

05

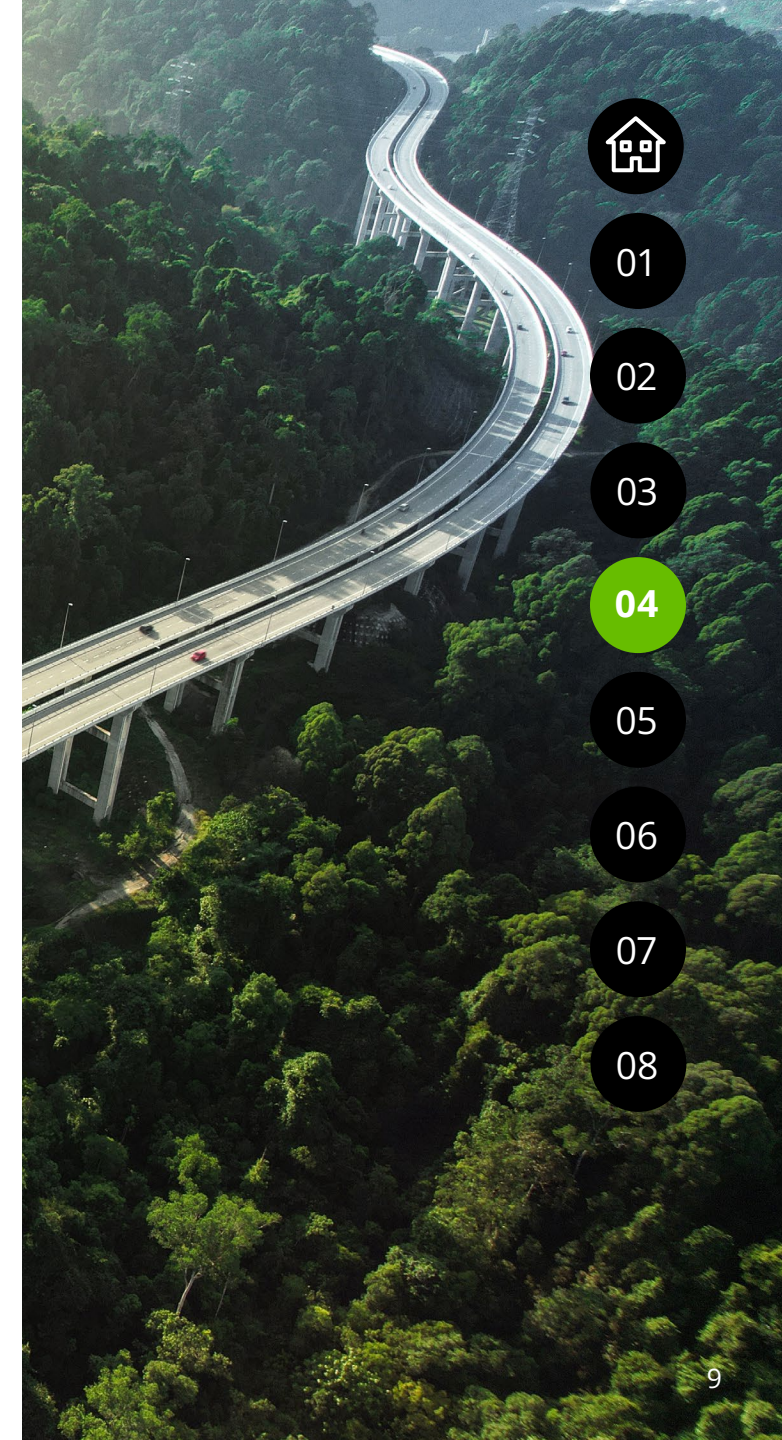
06

07

08

Common SOC readiness pitfalls—and ways to reduce them (cont.)

- **Missing or incomplete documentation:** Controls may operate in practice, but outdated policies, inconsistent procedures, or poorly documented evidence can still result in exceptions. In addition, controls can fail if responsibility for execution, review, or evidence retention is not clearly assigned. This risk can be reduced by management establishing named control owners and reviewers for each control, having clear expectations for timing and documentation, and completing a documentation quality review before readiness testing begins.
- **Failure of management to validate remediation:** Organizations often implement corrective actions but do not test that the fixes operate effectively end to end. This gap may be closed by retesting remediated controls, reviewing evidence for completeness and sufficiency, and obtaining control-owner confirmation of remediation before you proceed into the examination.
- **Business and IT coordination gaps:** When business and IT aren't aligned, ownership can become unclear and system or process changes may get overlooked. This can be addressed through shared governance, regular working sessions, and a deliberate review and testing of recent and upcoming changes across both the business and technology teams that impact the scope of the examination.
- **Third-party and subservice provider dependencies:** Organizations may overlook controls performed by vendors, cloud providers, or other subservice organizations, which may create gaps in coverage or unclear responsibilities. Aim to address this by identifying third-party dependencies early and documenting relevant CSOCs and monitoring activities and controls.
- **An incomplete or immature control environment:** Readiness may reveal a larger truth—that controls aren't designed, executed, or documented well enough to result in a report without findings or qualifications. Rather than forcing an examination, consider pausing to address foundational gaps and strengthen the control environment before proceeding with the examination.





Leading practices for SOC examination readiness

While SOC readiness processes vary by organization, certain leading practices can improve readiness regardless of industry. At their core, these practices emphasize disciplined execution, clear accountability, and a shared understanding of the importance of the subject matter that will be the scope of the examination. Organizations are generally better positioned when they treat the review of key controls within SOC readiness as an ongoing, cyclical process that supports continuous improvement, rather than a one-time effort performed just prior to the examination.

Leaders also play an important role in shaping a successful readiness effort. By encouraging transparency and a learning mindset, leaders let teams know that readiness isn't a test, but rather an opportunity to identify gaps and strengthen the control environment. Teams are then more likely to raise issues early, speak candidly about process challenges and changes, and contribute to a more effective and sustainable control environment.

Planning should be practical, sequenced, and visible to stakeholders, and the following leading practices should be considered:

- **Define scope early:** Clearly document the in-scope systems, products, services, locations, processes, and applicable control (SOC 1) and/or trust services criteria (SOC 2) objectives at the start of readiness. Review that scope with business, IT, and relevant stakeholders, and align it to the system description and relevant criteria before detailed readiness work begins. This preparation may reduce rework, examination delays and can create a stronger foundation for control design and testing.



01

02

03

04

05

06

07

08

Leading practices for SOC examination readiness (cont.)

- **Review the history of any prior controls findings and build them into the readiness plan:** Begin by reviewing the history of prior control findings, including those identified through SOX, internal audit, regulatory reviews and previous audit examinations, as well as readiness assessment results, control testing results, and related management or internal audit recommendations. This broad review helps identify recurring issues and known areas of control weakness. These insights can then be incorporated into the readiness plan to enable early focus on the issues likely to impact the examination, potentially reducing the risk of repeating deficiencies and likely strengthening overall control maturity.
- **Identify relevant third-party and subservice organizations:** Determine third-party and subservice provider dependencies in the beginning of the readiness process. This includes documenting which controls are performed internally versus by service organizations to clarify ownership and accountability. Relevant CSOCs should also be noted and assessed to confirm they are addressed within the control environment and there are established monitoring activities for select third parties. Taking these steps early can help close coverage gaps, reduce ambiguity in responsibilities, and support a more complete readiness assessment.
- **Establish a clear liaison and request intake model:** Assigning a dedicated liaison or central coordinator helps create a single, consistent channel for managing service auditor requests, routing questions, confirming ownership, and tracking due dates. This can improve the flow of information between service auditors and internal stakeholders, reduce duplication and confusion, and give the organization better visibility into request status and pending actions to allow for agreed-upon timelines to be met.



01

02

03

04

05

06

07

08



Leading practices for SOC examination readiness (cont.)

- **Provide regular internal updates to maintain alignment and stakeholder engagement:** SOC readiness efforts are typically more effective when stakeholders receive regular updates on progress, upcoming activities, open risks, and unresolved findings. Frequent communication can help keep control owners, business leads, IT, security, and compliance teams aligned on expectations and timelines, while also reinforcing accountability for remediation activities.
- **Fully remediating identified gaps:** The focus during the readiness is not only on documenting remediation actions. Instead, management should evaluate whether each gap has been addressed in practice, supported by sufficient evidence, and tested before the examination begins. A disciplined remediation process can decrease the likelihood of entering the examination with unresolved deficiencies or controls that have been updated but have not yet demonstrated to be operating effectively. Finally, it's important for teams to understand the business value of readiness. When the importance is highlighted, organizations are often better positioned to secure timely access to the right people, processes, and documentation, reducing delays and rework during the examination process. Strong readiness not only supports a smoother examination, but it can also reinforce a more coordinated and sustainable control environment.



01

02

03

04

05

06

07

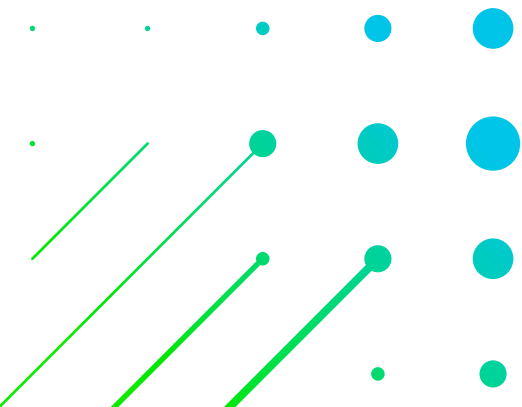
08



Deloitte's Third-Party Assurance (TPA) Readiness SelfAssess™ tool

For clients preparing for readiness, Deloitte offers a [TPA Readiness SelfAssess™](#) that organizations can use to self-evaluate their controls. It provides a practical starting point for strengthening your compliance efforts in alignment with leading frameworks.

The tool can perform a pre-assessment to determine your maturity to embark on SOC readiness assessments. It also identifies leading practices and surfaces what you're doing well, which areas may require additional focus, and what you should consider to potentially accelerate future remediation.



- 
- 01
- 02
- 03
- 04
- 05
- 06
- 07
- 08



Industry-leading advice for SOC readiness

After completing a self-assessment, organizations can engage Deloitte for a readiness assessment. Deloitte is a leading provider of SOC services in the United States, issuing approximately 800 SOC reports and performing nearly 490 readiness assessments each year for clients ranging from first-time reporters to Fortune 100 companies. Of these, we performed approximately 80 SOC specific readiness assessments. Our team includes more than 3,000 US Audit & Assurance professionals with experience in internal controls, cybersecurity, risk management, and information systems.



Get in touch

For more information about our Third-Party Assurance Services, contact us:

Authors



Kim Dragovic
Audit & Assurance Principal |
Deloitte & Touche LLP
kdragovic@deloitte.com





This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

The services described herein are illustrative in nature and are intended to demonstrate our experience and capabilities in these areas; however, due to independence restrictions that may apply to audit clients (including affiliates) of Deloitte & Touche LLP, we may be unable to provide certain services based on individual facts and circumstances.

About Deloitte

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2026 Deloitte Development LLC. All rights reserved.