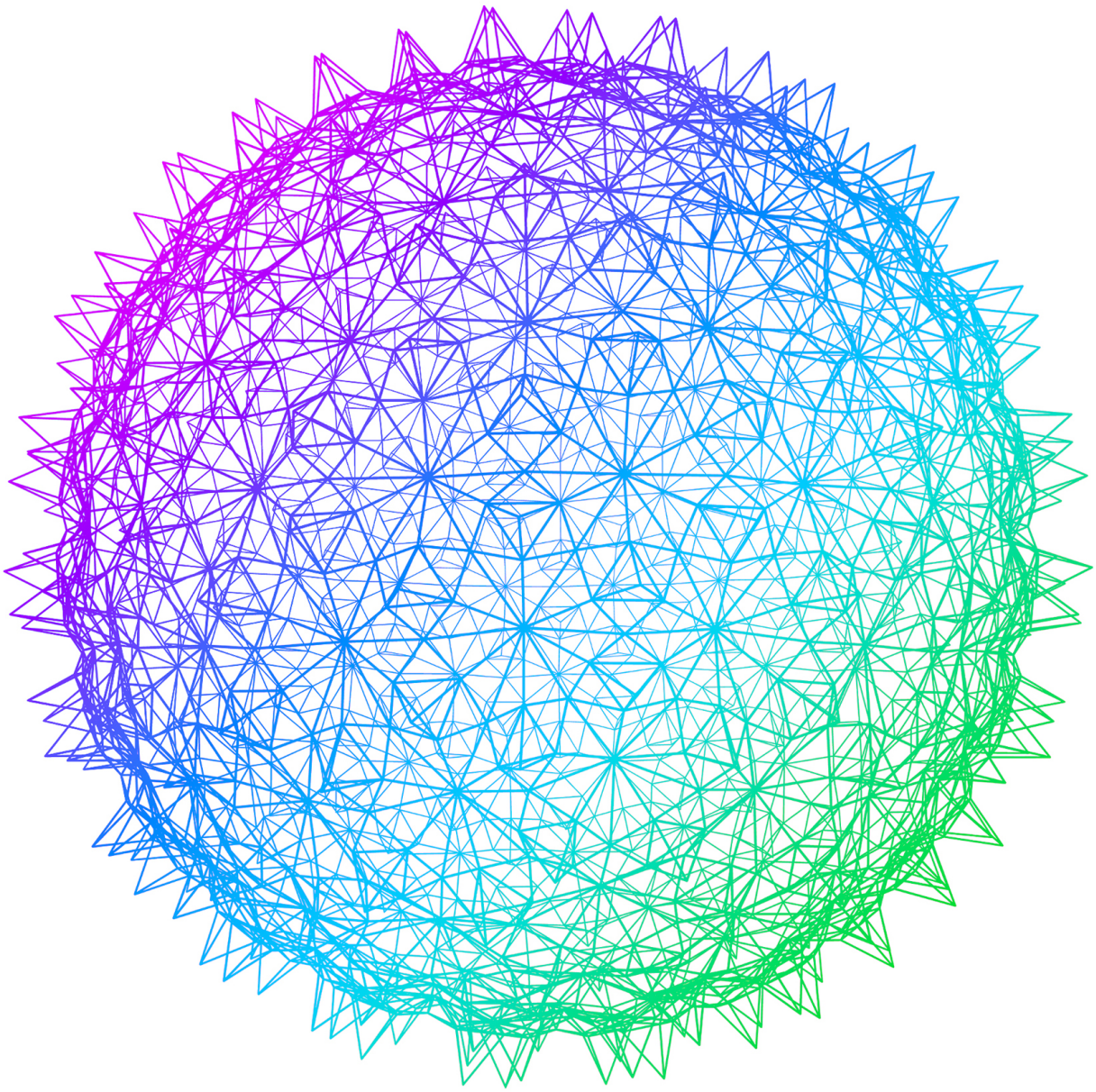
Deloitte.



Third-party reporting proficiency with SOC 2+

An integrated approach gains traction

Contents

Overview

Doing business as an "extended enterprise" is now the norm. Today, companies of all sizes routinely rely upon an ecosystem of service organizations to carry out a wide array of functions, many of them mission-critical. Through these loosely coupled networks of third parties, companies have been able to vastly expand their reach and capabilities, often extending around the world to create new and exciting market opportunities. At the same time, their increasing reliance on service organizations is fueling concern over greater enterprise risk exposure, especially since third-party risk is difficult to identify, manage, and monitor. For service organizations, this translates into increasing customer demand for system and organization control (SOC) reports.

These third-party assurance reports help service organizations build confidence in their service delivery processes and controls through the attestation of an independent certified public accountant.

Most organizations today are familiar with both SOC 1 and SOC 2 reports. While SOC 1 reports cover internal control over financial reporting (ICFR) and support a customer's financial audit, SOC 2 reports focus on the controls that are relevant to the following Trust Services Criteria (TSC) as established by the American Institute of Certified Public Accountants (AICPA):

Security

- Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.

Availability

- Information and systems are available for operation and use to meet the entity's objectives.

Processing integrity

- System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Confidentiality

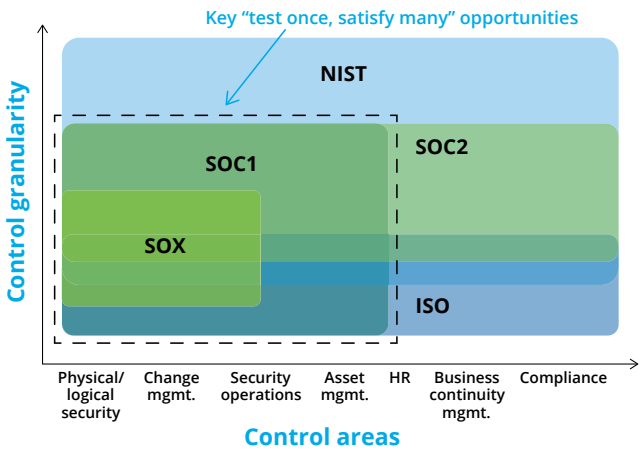
- Information designated as confidential is protected to meet the entity's objectives.

Privacy

- Personal information is collected, used, retained, disclosed, and disposed to meet the entity's objectives.

In recent years, as organizations have sought better ways to manage their risks from external relationships, many have implemented requirements for SOC 2 reporting directly into their service organization contracts to support due diligence when first establishing third-party relationships and for use as a monitoring mechanism. As a result, we've seen a large increase in demand for SOC 2 reports. In our experience, they now comprise about one-third of all third-party assurance reports requested by service organizations. Enhanced SOC 2 reports, also called SOC 2+ reports, are in particular demand. These reports are being used to demonstrate assurance in areas that go beyond the TSC, including compliance with a wide range of regulatory and industry frameworks such as those sponsored by the National Institute of Standards and Technology (NIST) and the International Standardization Organization (ISO), among others (see figure 1).

Figure 1. SOC 2: Entering a more expansive territory for reporting

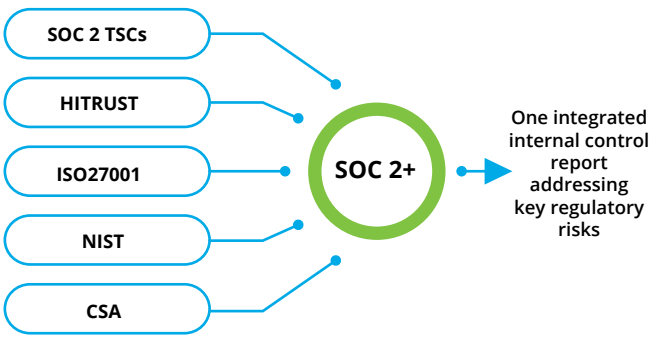


SOC 2+ reports: A way for service organizations to highlight their integrated controls

Providing assurance with regard to the TSC may be sufficient for some service organization customers, but others may require greater coverage. In particular, those within industries such as health care and financial services have additional industry-specific regulations and requirements. This is why the SOC 2+ concept was created. It is an extensible framework that allows service auditors to incorporate various industry standards into an SOC 2 report.

This integrated approach has been rapidly embraced by many service organizations and their customers. For instance, when creating SOC 2+, the AICPA collaborated with the Health Information Trust Alliance (HITRUST) to develop an illustrative SOC 2+ that incorporated criteria from the HITRUST Common Security Framework. Today, an SOC 2+ report is often the preferred means of pursuing HITRUST certification for service organizations with health care customers. The AICPA also collaborated with the Cloud Security Alliance (CSA) to develop a third-party assessment program for cloud providers. Called the Security Trust & Assurance Registry (STAR) Attestation, this framework combines SOC 2 attestation with the CSA's Cloud Controls Matrix (CCM), and it, too, is rapidly being embraced.

Figure 2. SOC 2+ reports can incorporate multiple frameworks



SOC 2+ reports are highly flexible tools that can incorporate multiple frameworks and industry standards into third-party assurance reporting (see figure 2). This flexibility can create substantial efficiencies for service organization customers, including reducing the amount of resources required for third-party oversight. Because SOC 2+ reports are based on a common control framework and address various industry standards, organizations generally do not have to spend as much time and effort conducting performance reviews at their service organizations. Organizations, as well as their service organizations, are also less likely to be exposed to compliance violations that can result in various forms of liability, including fines. For these reasons, some organizations have begun to stipulate their preference for using integrated frameworks as a means of obtaining third-party assurance by writing it into their service organization contracts.

Though customers can benefit greatly from SOC 2+ reports, the advantages for service organizations are even more significant. Consider that these businesses often must respond annually to hundreds of individual audit requests, customer questionnaires, and requests for proposals. Many of these inquiries ask the same questions and demand assurance on overlapping controls. Throw regulatory and industry-specific requirements into the mix, and things get even more complicated and onerous.

SOC 2+ examinations can dramatically reduce this burden. By providing a standardized format for meeting a broad range of regulatory and industry control requirements, SOC 2+ reports help to eliminate the need for redundant activities and one-off responses. Through a single examination based on the AICPA TSC and one or more integrated frameworks, they allow service organizations to demonstrate to their customers and other stakeholders that effective internal controls are in place (see table 1). SOC 2+ reports can also be tailored to meet the ever-growing list of security questionnaires by mapping to suitable and available criteria that can help provide customers with trust and confidence that they are achieving the concepts in the questionnaire.

Table 1. Incorporating some common frameworks into SOC 2+

Framework	Description	SOC 2+ example
HITRUST	This framework supports the Health Insurance Portability and Accountability Act (HIPAA), the US government's security standards that all health plans, clearinghouses, and providers must follow. Standards are required at all stages of transmission and storage of health care information to help ensure integrity and confidentiality.	A service organization claims processor must have access to HIPAA data in order to execute its responsibilities. To demonstrate that it is adequately safeguarding personal health information, it mapped its controls to the HITRUST framework.
National Institute of Standards and Technology (NIST)	The NIST framework focuses on improving cybersecurity for critical infrastructure.	A company that maintains governmental contracts for building roads and bridges has contractual obligations to demonstrate how it meets the latest revision of NIST.
Cloud Security Alliance (CSA)	CSA, in collaboration with the AICPA, developed a third-party assessment program of cloud providers officially known as CSA Security Trust & Assurance Registry (STAR) Attestation.	A cloud provider possesses its clients' information in both public and private clouds, which has unique security implications. Accordingly, it has to address the CSA Cloud Controls Matrix (CCM) and provide sufficient documentation to apply for the STAR Attestation certification.
International Organization for Standardization (ISO) 27001	ISO 27001 is the international standard for securing information assets from threats and provides requirements for broader information security management.	A data center provider has data centers and clients around the world. It continues to get security questionnaires and requests for understanding how it manages security. Rather than addressing each questionnaire individually, the center chooses to compile an SOC 2+ mapped with ISO 27001 to demonstrate its information security controls.

Journeying from SOC 2 to SOC 2+

SOC 2+ reports call for a different way of organizing requirements and testing controls, which may take some getting used to. Yet businesses with regulatory or industry framework requirements that want to become truly proficient in its approach to third-party reporting will need to consider issuing an SOC 2+ report sooner or later. Demonstrating compliance with a wide variety of frameworks within a single document simply makes more sense than approaching each request for assurance separately. To make the journey from SOC 2 to SOC 2+ easier and more effective, here are some guiding principles culled from our experience in performing SOC 2+ attestations.

Start small

Nailing down the basic SOC 2 report is an important first step. Generally, service organizations have a certain degree of leeway when it comes to designing their SOC 2 reports. In fact, most contracts are somewhat vague (i.e., they don't specify which TSC(s), or which systems, should be tested). With this in mind, a leading practice is to limit the initial reporting scope to only those systems or criteria required to support the scope of the description of the system, emphasizing those that are most important to customers. Once the organization is confident about the controls surrounding this subset, it can then branch out, mapping and testing the controls relevant to a broader range of customer needs.

In considering how to proceed, assurance with regard to the security TSC, which forms the basis of all SOC 2 reports, is a natural place to start, particularly since cybersecurity is vitally important to many customers. The most complex of the five is the privacy TSC.

However, customers are becoming more concerned with service organizations' interactions with end users and related privacy practices. While saving privacy for last may make sense, it cannot be overlooked. Ultimately, it may need to be addressed for compliance purposes if a service organization interacts directly with end users and gathers or stores their personal information. Given the complexity of the privacy criterion, it can be wise to get help. SOC 2 privacy reports do require more effort, and service organizations often need readiness assistance to complete them.

Know your customer

Every customer has different requirements. While contracts may be somewhat vague concerning the specifics of SOC 2 reporting, service organizations shouldn't assume they know what a customer is looking for without first confirming it. For example, issuing an SOC 2 report on Application A and its associated processes, when the customer really wanted Application B to be examined, will result in wasted resources and a lot of rework. These costly misunderstandings happen far too often, especially when they can be avoided through better communication and greater insight into customer needs.

For many service organizations, understanding what their customers are looking for often comes down to educating the salesforce and other customer touchpoints about SOC 2 reporting. When customer-facing personnel grasp the value of an integrated approach, they can both communicate the benefits and ask customers the right questions to help scope and define their requirements. Making the effort up front to probe customer requirements—not only the what, but also the why—will both save time in the long run and build customer confidence and trust.

Furthermore, many customers may be unaware that it's possible to combine SOC 2 with other compliance initiatives, such as HIPAA or NIST, when requirements overlap. This gives service organizations a great opportunity to add value by showing customers how SOC 2+ can be used to streamline reporting processes. This can be accomplished through the following steps:

- To begin, compile a list of requirements for each TSC.
- Then move on to a list of requirements for each of the other frameworks with which your customers must comply.
- From there, identify areas where similar operational controls will meet both SOC 2 and other requirements.
- Subsequently, create a master list of the integrated requirements by mapping them to one another. This allows for testing each control once, then "checking the box" for all of the requirements to which it applies.

Organize and plan

If an organization hasn't previously considered issuing an SOC 2+ report, then most likely external or independent auditors haven't tested its integrated compliance controls before. Also, it is not uncommon for service organizations, particularly those subject to Sarbanes-Oxley (SOX) Section 404, to focus their control efforts primarily on ICFR. If so, they may not have applied that same level of rigor to the controls for their operational systems. For these reasons, a readiness assessment, performed by an independent third party, is often well worth the effort. This includes inspecting the controls that are already designed and implemented, as well as identifying any gaps or deficiencies that will need to be addressed prior to live testing.

A readiness assessment can ultimately save time and effort by:

- Identifying problems before they need to be reported;
- Leveraging subject matter experts to document controls; and
- Defining the correct scope and boundaries of the system up front.

In our experience, service organizations that don't complete a readiness assessment tend to have more issues during the actual examination.

Build on your success

Once the necessary controls and procedures are in place for SOC 2, an organization can start integrating other frameworks. Individual controls will invariably fulfill multiple requirements. For example, a control that meets one of the requirements of an SOC 2 Security TSC may also meet certain NIST and ISO 27001 security requirements (see table 2). Mapping these redundancies greatly facilitates testing efficiencies when seeking to comply with multiple industry-specific or regulatory requirements.

Table 2. Example of SOC 2+ control mapping

NIST activity	ISO 27001 control #	Trust services criteria	Control activity	Test procedures	Test results
The organization: • Separates by assigning defined duties to individuals. • Documents separation of duties (SoD) of individuals. • Defines information system access authorizations to support SoD.	A.9.2.2. A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services. A.9.2.3 The allocation and use of privileged access rights shall be restricted and controlled.	CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	A documented security policy outlines SoD among key business groups. Access requests are run through a governance, risk, and compliance (GRC) system to help validate that SoD hasn't been violated, and results of that validation are maintained within the user's access request ticket.	Obtained the access control policy and procedures to ascertain if they have been updated periodically and include defined processes for SoD. Inspected a sample of user access additions and changes and determined that the access requests had been run through the GRC tool to document that SoDs had been evaluated.	No exceptions noted.

Rapidly gaining traction

The complexity of the extended enterprise has exposed both service organizations and their customers to many risks that could be difficult to mitigate. On one hand, organizations that outsource important and mission-critical functions need assurance that their providers have rigorous control processes in place. On the other hand, service organizations need a way to streamline the ways in which they provide that assurance. SOC 2+ reports are rapidly gaining traction as the preferred method of addressing these concerns because they provide an efficient approach to organizing, testing, and reporting on controls for multiple frameworks simultaneously.

Service organizations that use SOC 2+ reports adeptly may gain a competitive advantage over other providers that are less proficient in their approaches to third-party reporting. And, perhaps best of all, by using SOC 2+ reports to facilitate information exchange, everybody wins, as members of the extended enterprise gain the insight needed to better manage risk together.

Did you know?

SOC 2+ reports can help businesses to obtain HITRUST certification. HITRUST is a not-for-profit organization whose mission is "to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain."[1] At the core of the organization's work is the HITRUST Common Security Framework (CSF), which rationalizes health care–relevant regulations and standards, such as NIST, HIPAA, and PCI-DSS, into a single, certifiable controls framework. Service organizations with health care customers increasingly have contractual obligations to become HITRUST certified, or at least to demonstrate that they are using a standard security framework, such as the HITRUST CSF. While many hold the HITRUST framework in high regard, fewer are familiar with how to get certified and the benefits of doing so.

While providers can pursue certification through the HITRUST CSF Assurance program, an SOC 2+ engagement carried out by an independent auditor adds additional value in that it integrates the AICPA Trust Services Criteria and the HITRUST CSF and can be used for certification purposes. Not only can SOC 2+ be used to fulfill contractual obligations, but it can also be used as a competitive differentiator. In a crowded field where it is hard to stand out, organizations can share the SOC 2+ with their customers to set themselves apart from those who have not met such rigorous controls standards.

Case in point: Multinational cloud provider

Deloitte helped a multinational cloud provider, which operates throughout the entire cloud stack, to integrate and rationalize the necessary frameworks. The biggest challenge for the engagement team came in identifying the differences between SOC 2 criteria and the CSA CCM and German C5 requirements.[2] Though it wasn't a big leap to identify the types of safeguards that would be needed, in-depth knowledge was required to spot the differences between the frameworks and to provide guidance on how to address them using existing controls. In some instances, this simply involved asking the right questions and documenting the controls that were already in place. In others, it required specialized knowledge, whereby engagement team members had to have certain professional certifications, along with three years of audit experience, in order to meet the requirement of the frameworks and provide the necessary level of technical depth. Through the resulting SOC 2+ report, the organization found a more efficient way to comply with multiple security requirements while gaining the documentation needed to apply for the desired certifications.

Case in point: Software-as-a-service platform

A company that mainly focused on providing a secure, cloud-based communication and content-sharing platform to financial services entities sought to expand into adjacent markets, such as health care and insurance. As a software-as-a-service (SaaS) provider, the organization needed a way to give its customers comfort about their controls around system security, platform availability, and data confidentiality. While these objectives could be met through a traditional SOC 2 report, the company had the additional goal of helping ensure prospective customers that they would be able to use the systems immediately without any concern about HIPAA requirements. For this reason, it chose to integrate the Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) into an SOC 2 engagement. Deloitte assisted the company by first performing a readiness assessment and identifying controls that would need to be added to the SOC 2 criteria in order to comply with the HIPAA Security Rule. It then audited the company's controls and issued an opinion via an SOC 2+ report. At present, the SOC 2+ report is widely seen as one of the most effective ways to demonstrate having controls over HIPAA data because there is no official HIPAA certification process. In this instance, the SOC 2+ engagement effectively reconciled two distinct business objectives: It not only addressed the third-party assurance concerns of the company's financial services customers, but also paved the way for growing the business into other sectors.

Case in point: Financial technology solutions

Offering a broad range of products for moving and managing money, a global leader in financial technology solutions found that it had to comply with multiple industry-specific security requirements. In addition to meeting the standards established by NIST, the company also sought to comply with the Federal Information Security Management Act (FISMA), as well as to become HITRUST certified. With competing demands for third-party assurance, the company decided to take an integrated approach to fulfilling its customers' complex reporting demands. With Deloitte's assistance, the company embarked on an SOC 2+ engagement that incorporated several frameworks into a single report.

The company chose Deloitte largely due to its ability to assemble an experienced multidisciplinary team, including federal practitioners with detailed FISMA knowledge. By addressing all of the requirements at once and helping to eliminate redundancies, the ensuing SOC 2+ report saved the company a great deal of time and resources while allowing it to apply for the certifications needed to grow its business across industries. The company also uses the report as its first line of defense in responding to security questionnaires, thus generating additional efficiencies and further compounding the benefits of taking an integrated approach to third-party assurance reporting.

Endnotes

1. HITRUST Alliance, "About HITRUST."
2. Refers to Bundesamt für Sicherheit in der Informationstechnik (BSI) Cloud Computing Compliance Controls Catalogue, which is commonly known as "C5."

Contact us

Curtis Stewart
National Third-Party Assurance Leader
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 703 251 1782
custewart@deloitte.com

Dan Zychinski
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 404 220 1169
dzychinski@deloitte.com

Alan West
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
+1 402 444 1807
alwest@deloitte.com

Deloitte.