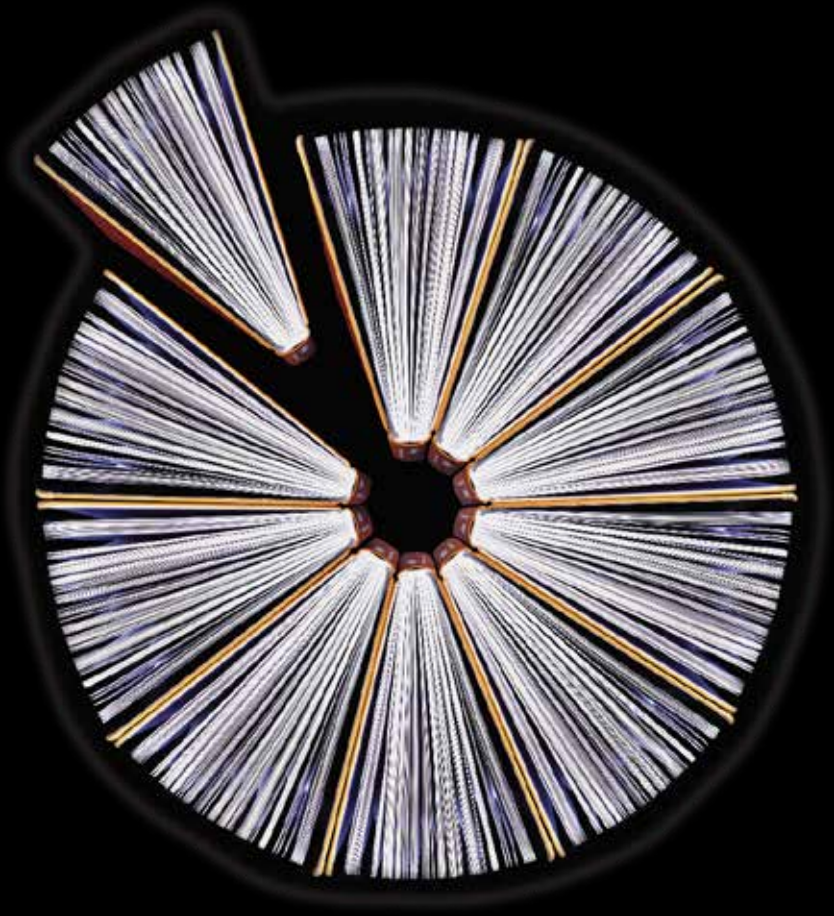
Deloitte.



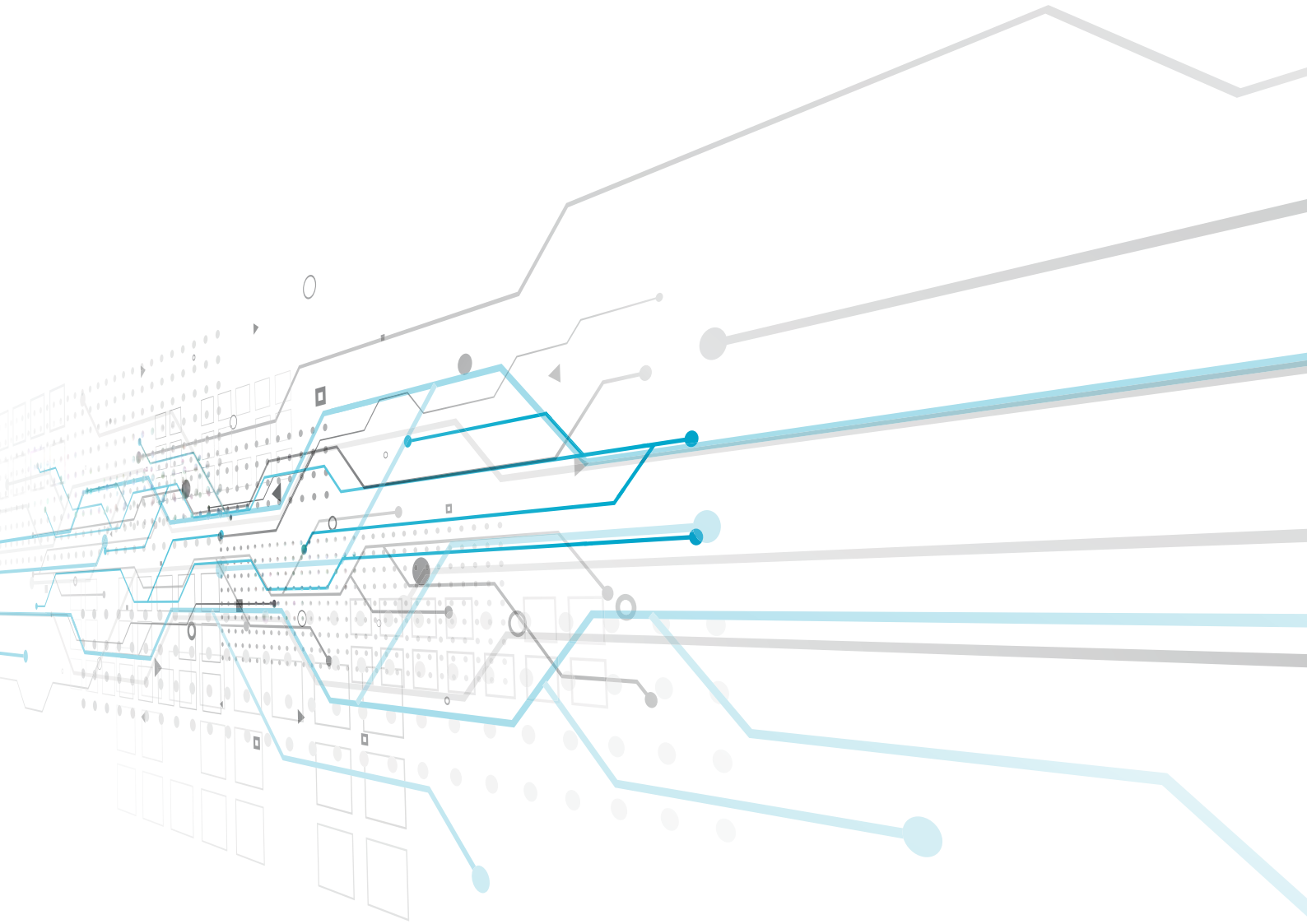
Achieving third-party reporting proficiency with SOC 2+

For private circulation only

October 2018

Risk Advisory

Contents



Achieving third-party reporting proficiency with SOC 2+

Today's organizations do business within a broad ecosystem. Customers, partners, agents, affiliates, vendors, and service providers make up an "extended enterprise" of third parties, many with operations around the world. The extended enterprise gives companies access to a broad range of capabilities, creating new and exciting market opportunities. At the same time, it has altered how organizations must assess and manage enterprise risk. The growing use of outsource service providers (OSPs) to carry out a wide array of functions, many of them mission-critical, has fueled concern over greater enterprise risk exposure.

Increased reliance on OSPs exposes organizations to risks that are difficult to identify, manage, and monitor. This has prompted organizations to demand that OSPs provide them with Service Organization Control (SOC) reports. These third-party assurance (TPA) reports help OSPs build trust and confidence in their service delivery processes and controls through the attestation of an independent certified public accountant.

Most organizations that work with OSPs are familiar with SOC 1 reports, which cover internal controls over financial reporting (ICFR) and support a customer's financial audit. SOC 2 reports, on the other hand, enter a more expansive territory (see Figure 1), focusing on the OSP's controls that are relevant to American Institute of Certified Public Accountants' (AICPA) Trust Service.

Principles (TSPs):

01 **Security:** The system is protected against unauthorized access (both physical and logical). The security TSP serves as the basis for all SOC 2 reports and is commonly referred to as the Common Criteria.

02 **Availability:** The system is available for operation and use as committed or agreed.

03 **Processing integrity:** System processing is complete, accurate, timely, and authorized.

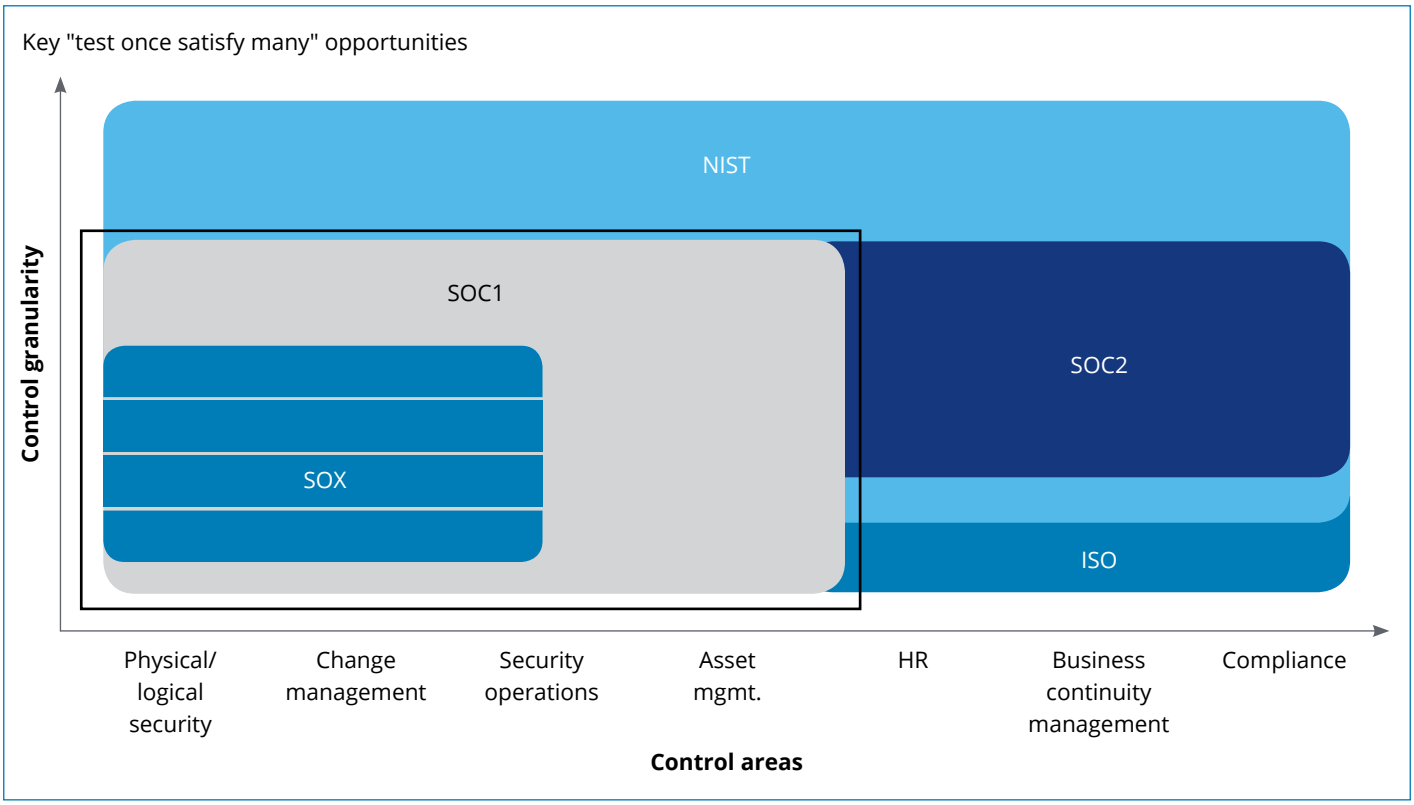
04 **Confidentiality:** Information designated as confidential is protected as committed or agreed.

05 **Privacy:** Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice.

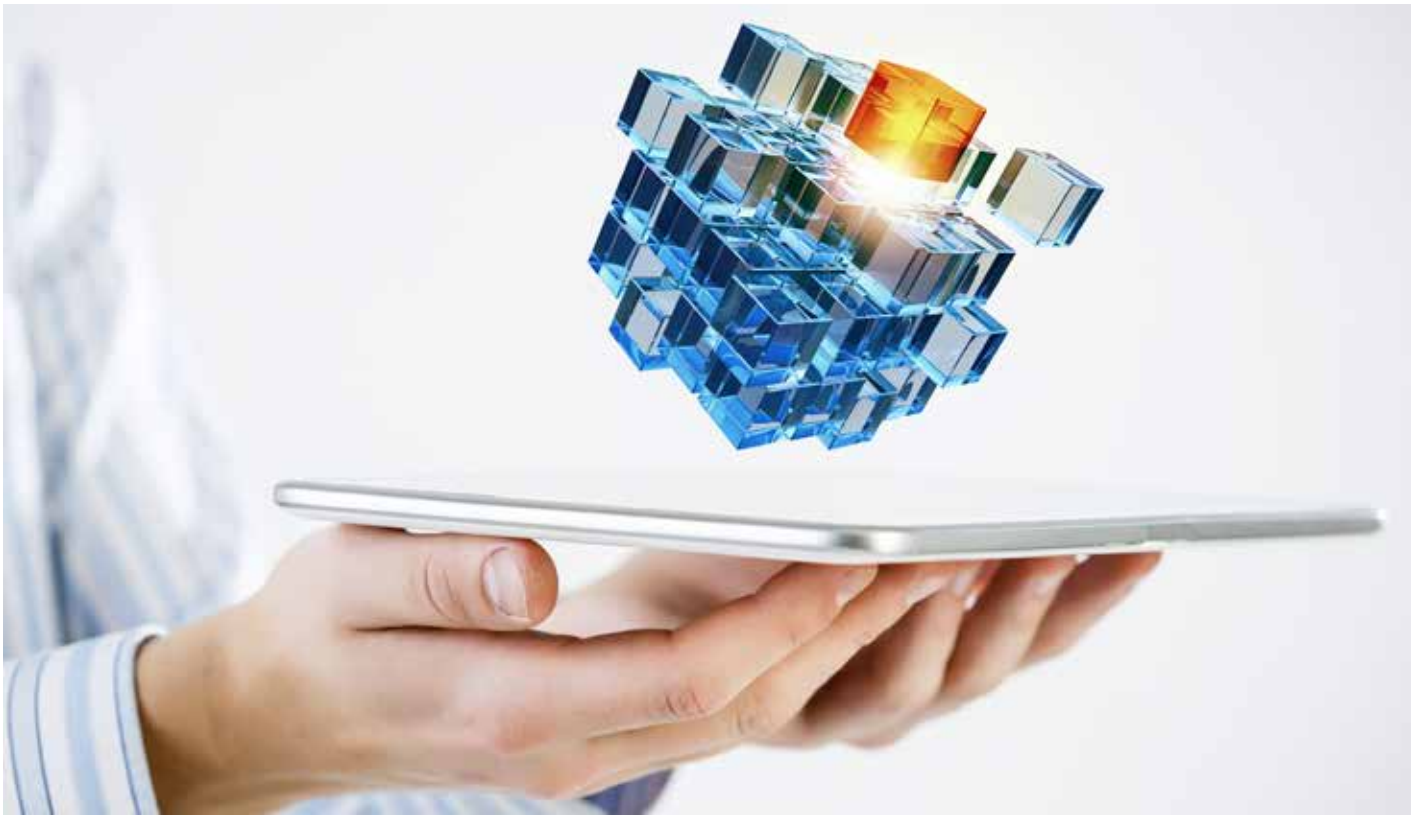
As organizations outsource more of their core operational functions, they are building requirements for SOC 2 reporting directly into their OSP contracts. As a result, we've seen a large increase in demand for SOC 2 reports: they now comprise approximately one- third of all TPA reports requested by OSPs.

In particular demand are enhanced SOC 2 reports, also called SOC 2+ reports. These reports can be used to demonstrate assurance in areas that go beyond the TSPs to include compliance with a wide range of regulatory and industry frameworks such as the National Institute of Standards and Technology (NIST), the International Standardization Organization (ISO), etc.

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



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



Providing assurance with regard to the TSPs may be sufficient for some OSPs' customers. But others may require greater detail. In particular, those in industries such as health care and financial services have additional industry-specific regulations and requirements. For this reason, the AICPA has created SOC 2+. This extensible framework allows OSPs' auditors ("service auditors") to incorporate various industry standards into a SOC 2 report. For example, the AICPA collaborated with the Health Information Trust Alliance (HITRUST) to develop an illustrative SOC 2+ that incorporates criteria from the HITRUST Common Security Framework (CSF). 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.1

SOC 2+ reports are highly flexible tools that can incorporate multiple frameworks and industry standards into third-party assurance reporting (see Figure 2).

SOC 2+ reports create substantial efficiencies for organizations. These reports are based on a common control framework and address various industry standards. Therefore, organizations are able to spend less time and fewer resources conducting performance reviews at their OSPs. Both OSPs and

customers are also less likely to be exposed to compliance violations that can result in various forms of liability, including fines. This can pave the way for contracts to start specifying integrated framework demands as a way for providing organizations with assurance.

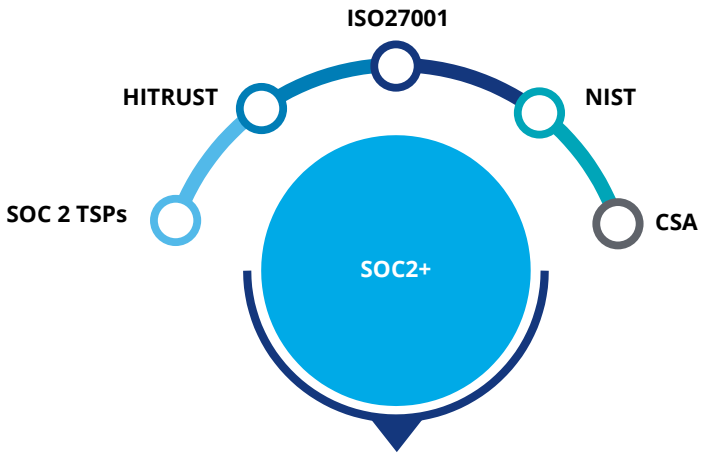
For OSPs, the benefits are even more significant. Consider that these businesses must often respond annually to hundreds of individual audit requests, customer questionnaires, and requests for proposals. Many of these requests require a separate analysis and response to the same or overlapping questions.

Throw regulatory and industry-specific requirements into the mix, and things get even more complicated and onerous.

SOC 2+ reports are a multifaceted and adaptable tool that allow OSPs to demonstrate to organizations and other stakeholders that effective internal controls are in place. These controls pertain to the criteria covered in the TSPs of security, availability, processing integrity, confidentiality, and privacy, as well as many of the more detailed requirements covered in other regulatory and industry-specific frameworks.

They offer a standardized format for meeting a broad range of regulatory and non-regulatory control requirements, eliminating the need for redundant activities and one-off responses. They're also flexible enough that they can be tailored to meet the specific needs of organizations. Table 1 lists some illustrative frameworks that could be incorporated into a SOC 2+ and the type of OSPs that could benefit from adding these to their SOC 2 examinations.

Figure 2: SOC 2+ reports can incorporate multiple frameworks



One integrated internal control report addressing key regulatory risks

Table 1: Incorporating multiple frameworks into SOC 2+

Framework	Description	SOC 2+ example
HITRUST (Health Information Trust Alliance)	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 ensure integrity and confidentiality.	An OSP 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 maps its controls to the HITRUST framework.
NIST (National Institute of Standards and Technology)	The NIST Framework focuses on improving critical infrastructure cybersecurity.	A company that maintains governmental contracts for building roads and bridges has contractual obligations to demonstrate how it meets the latest revision NIST.
PCI-DSS (Payment Card Industry – Data Security Standard)	This is a proprietary standard for organizations involved in the storage, processing and/or transmission of cardholder data (CHD).	An OSP payment processor stores credit card information for future payments. Its customer want to know the details of the OSP's controls beyond the PCI certification. In situation where there is no PCI certification, there is a need to demonstrate what controls are in place.
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 data center provider possesses its clients' information in both public and private clouds. Due to the unique security configurations, its clients have required a SOC 2+ with STAR
ISO27001	ISO 27001 is the international standard for securing information assets from threats and provides requirement 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 a 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. Therefore, moving from issuing SOC 2 to the more versatile SOC 2+ reports may take some getting used to. Yet any business that wants to become truly proficient in its approach to third-party reporting should look at ways to demonstrate compliance with a wide variety of frameworks within a single document. There are a number of guiding principles that will make the journey from SOC 2 to SOC 2+ easier and more effective.

Start small

Nailing down the basic SOC 2 report is an important first step. Generally, OSPs have a certain degree of leeway when it comes to designing their SOC 2 reports. In fact, most contracts are somewhat vague— they don't specify which TSPs, or which systems, should be tested. We therefore recommend focusing initial reporting scope on a subset of environments or a subset of TSPs—the principle or principles that are most important to customers. Once you're confident about the controls surrounding a limited set of TSPs and environments, you can then branch out, mapping and testing the controls relevant to a broader set of customer needs.

Assurance with regard to the security TSP is more or less a given, so this is the optimal starting point. Furthermore, as cybersecurity becomes increasingly critical, this TSP is likely to become even more important to customers. The most complex of the five is the privacy TSP. Yet with the increase in data breaches, privacy has moved front and center as a concern for many customer organizations. While saving privacy for last may make sense, ultimately it needs to be addressed if an OSP interacts directly with end users and gathers their personal information. SOC 2 privacy reports do require more effort, and OSPs may require outside assistance to complete them.

Know your customer

Every customer has different requirements. While contracts may be somewhat vague when it comes to the specifics of SOC 2 reporting, don't assume you know what a customer is looking for without first confirming it. For example, issuing a SOC 2 report on "Application A" and its associated processes, when your customer had really wanted you to be testing "Application B," will only result in wasted resources and a lot of re-work. Understanding customer needs ultimately comes down to educating your salesforce and other customer touchpoints. When they understand SOC reporting, they can both communicate the benefits and ask customers the right questions to help scope and define their requirements. Taking the time up front to probe customer requirements—not only the what, but the why—will save you time in the long run and increase customer confidence and trust.

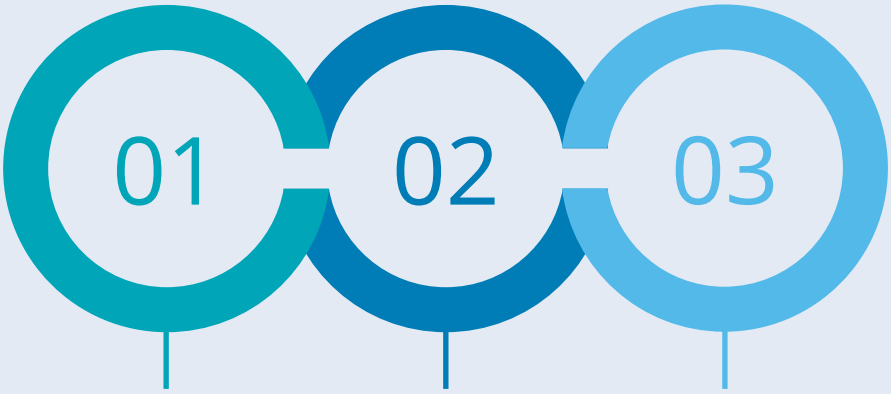
Many customers may be unaware that it's possible to combine SOC 2 with other compliance initiatives, such as HIPAAor NIST, when requirements overlap. This gives you an opportunity to show customers how to achieve greater reporting efficiencies. Start with a list of requirements for each of the TSPs and those for other frameworks with which your customers must comply. At the beginning of the engagement identify areas where similar operational controls will meet both SOC 2 and other requirements and create a master list of the integrated requirements by mapping them to one another. This will allow you to test each control once and then "check the box" for all the requirements to which it applies.

Organize and plan

If this is your first time compiling a SOC 2+ report, then most likely compliance controls haven't been tested by external or independent auditors in the past. It's not uncommon for OSPs, particularly those subject to Sarbanes-Oxley Section 404 (SOX), 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.

We therefore recommend performing readiness testing on these systems to determine whether controls are robust enough to meet the appropriate TSPs or various SOC 2+ framework requirements during an actual examination. In our experience, OSPs that don't prepare in advance tend to have more issues with controls during actual testing.

Readiness consists of having an external auditor come in and perform an assessment of the control environment. This includes identifying the controls that are already designed and implemented, as well as any control gaps or deficiencies that will need to be addressed. 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

Defining the correct scope and boundaries of the system up front

Build on your success

Once you feel that you have the necessary controls and procedures in place for SOC 2, you can begin to integrate other frameworks. Individual controls invariably fulfill multiple requirements. For example, a control that meets one of the requirements of a SOC 2 Security TSP may also meet a particular NIST and ISO27001 security requirement (see Table 2). When organizations need OSPs to demonstrate compliance with various industry-specific or regulatory requirements, in addition to general compliance with the TSPs, mapping redundant requirements will greatly facilitate testing efficiencies (see Figure 3).

Figure 3: Steps to third-party proficiency

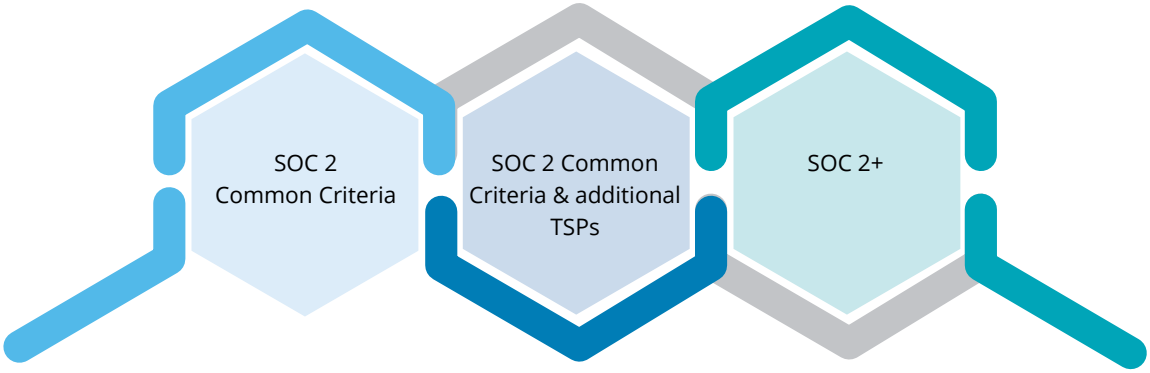


Table 2: Example of SOC 2+ control mapping

NIST Activity	ISO 27001 control #	Trust Service Principle criteria	Control activity	Test procedures	Test result
The Organization; • Separates Assignment organization defined duties of individual. • Documents separation of duties (SoD) of individuals. • Defines information system access authorizations to support separation of duties.	A.10.1.3	Common Criteria 5.1: Common Criteria 5.4:	A document security policy outlines SoD among various key business groups. Access requests are run through a GRC system to validate that SoD isn't 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 the policies were updated on a periodic basis and included defined processes for SoD. Inspected a sample of user access additions and changes and ascertained that their access requests were run through the GRC tool to document that SoDs were evaluated.	No exceptions noted.

Forging into new territory

The complexity of the extended enterprise has exposed Organizations too many risks that are outside their control. Organizations that rely on OSPs for important and mission critical functions need assurance that OSPs have rigorous control Processes in place. Furthermore, as regulations proliferate, OSPs and their customers alike must be able to utilize an integrated internal control report with a wide range of industry-specific and other requirements. SOC 2+ reports are an efficient approach to organizing, testing, and reporting on controls for multiple frameworks simultaneously. Outsourcers that have a streamlined process for delivering these reports to customers may find themselves with a significant advantage in demonstrating their third-party proficiency. When OSPs and organizations work together, SOC 2+ reports can become an efficient exchange of information in the marketplace.

Contact

Rohit Mahajan
President
Risk Advisory
rmahajan@deloitte.com

Deepa Seshadri
Partner
deseshadri@deloitte.com

Kedar Sawale
Partner
ksawale@deloitte.com

Ramu N
Partner
ramun@deloitte.com

Johar Batterywala
Partner
jobatterywala@deloitte.com

Deloitte.