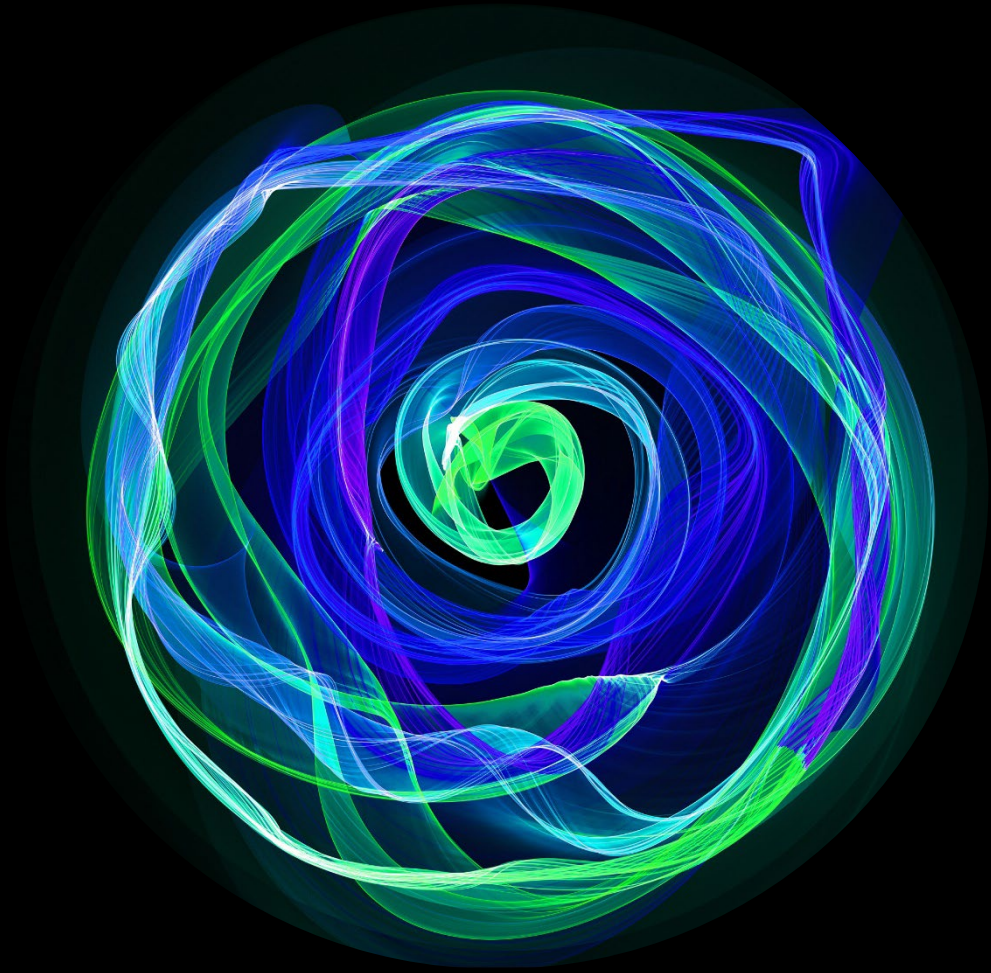


**Deloitte.**



Providing Assurance  
through SOC Reports






# Many companies rely on SOC 1 and SOC 2 reports to address Sarbanes-Oxley (SOX) and other compliance requirements.

Service organizations often find themselves serving many industries across multiple geographies, which expands the range of compliance and regulatory requirements they must meet.

Under increasing compliance pressures, companies are asking their service organizations to demonstrate the efficacy of their controls to higher degrees. In some cases, SOC reports have become a pre-requisite for service organizations to win new business with established companies.

According to the AICPA<sup>1</sup> & CIMA<sup>2</sup> 2020 SOC Survey, there is a growing market for SOC services with a 49% increase in demand for SOC 2 engagements between 2018 and 2020.

Let us take you through what you need to know about providing assurance to customers, business partners, regulators, and auditors through SOC reports.

-  How a SOC report works
-  Benefits of a SOC report
-  SOC 1 and SOC 2 comparisons
-  SOC 2 trust services categories
-  SOC 2 additional options
-  Components of a SOC report
-  Typical path for a new SOC report
-  SOC readiness assessment
-  Selecting your service auditor

# How a SOC report works

The System and Organization Controls (SOC) report framework was developed by the AICPA as part of the Statement on Standards for Attestation Engagements (SSAE) 18. An independent auditor performs procedures and issues an audit opinion, following similar independence requirements applicable for external audits over financial statements.

An **organization** provides services to customers and engages with an **independent service auditor** to examine and provide an opinion on their relevant internal controls.



## User entity

- Customers
- Business partners
- Regulators
- Auditors of user entity

## Benefits of a SOC report

- **Audit and Regulatory**  
May be used by user entities in support of regulatory and legal requirements, including SOX
- **Responding to Requests**  
May be leveraged to respond to internal control and audit requests from suppliers, customers, and their auditors
- **Control Environment**  
Brings focus on internal controls and control environment in accordance with COSO framework
- **Contracting**  
Assists in meeting contractual requirements for existing and prospective customers
- **Risk Management**  
Provides an opportunity to further enhance enterprise and third-party risk management and monitoring
- **Compliance**  
May be leveraged to provide assurance related to compliance with certain requirements specified by customers and government agencies

# SOC Report Comparisons

The most common third-party assurance reports are SOC 1 and SOC 2 reports.



## SOC 1

- Examination of controls relevant to internal control over financial reporting, intended to meet the needs of user entities evaluating for their user entity financial statements
- Customized control objectives and controls with consideration to services provided and related financial statement assertions
- Scope can be business or IT controls
- Issued in accordance with the AICPA's SSAE 18 standard



## SOC 2

- Examination of controls related to specific trust categories (security, availability, processing integrity, confidentiality, or privacy), service commitments, system requirements, and potentially compliance (SOC 2+)
- Standard trust services criteria (TSC) in which controls are identified and mapped to
- Scope is IT controls for specified products or services
- Issued in accordance with the AICPA's SSAE 18 standard and AICPA 2017 Trust Services Criteria



## Type 1 and Type 2 Reports

### Type 1

- Reports on an organization's description of controls, whether such controls were suitably designed and whether they had been placed in operation as of a specified date as of a point in time (e.g., as of June 30, 202X)
- Most often performed only in the first year of a SOC report

### Type 2

- Includes everything in the Type 1 report plus testing the operating effectiveness of controls over a specified time period (6-12 months)
- Includes a description of the testing procedures performed by the service auditor and the results of testing performed

# SOC 2 Trust Services Categories

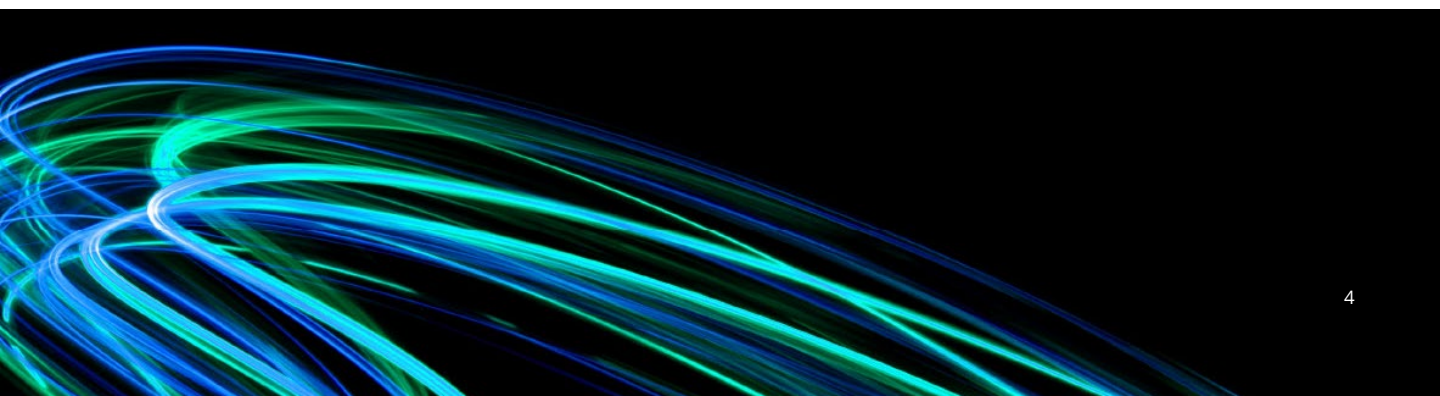
SOC 2 represents an examination on controls relevant to the following trust services categories, which are mapped to trust services criteria (“TSC”)

Trust Services Categories		Select TSC Required in all SOC 2 Reports (“Common Criteria”)	
Category	No. of TSC	Area	No. of TSC
<b>Availability</b> , addressing continuity of operations	3	Control Environment	5
<b>Processing Integrity</b> , including complete, accurate, and timely processing	5	Information and Communication	3
<b>Confidentiality</b> of information	2	Risk Assessment	4
<b>Privacy</b> as it relates to the collection, use, retention, disclosure, and disposal of personal information (PI).	18	Monitoring	2
<b>Security</b> against unauthorized access or appropriation, either logical or physical	33	Control Activities	3
		Logical and Physical Access Controls	8
		System Operations	5
		Change Management	1
		Risk Mitigation	2
		<b>Total</b>	<b>33</b>

Aligned with the 17 principles in the COSO framework

Other Required Common Criteria

*Note: Security is a required category mapped to common criteria; the remaining categories are optional*



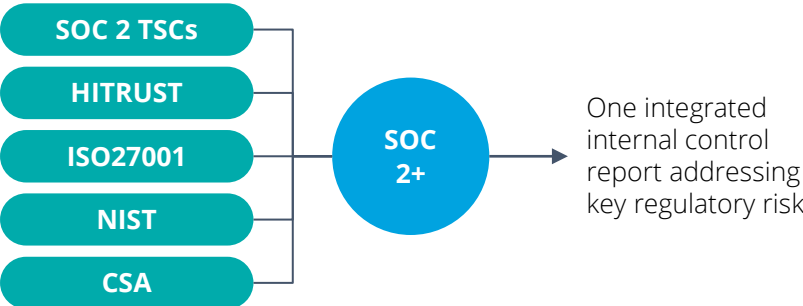


# SOC 2 Additional Options

## Adding Other Criteria (SOC 2+)

The AICPA has provided a great deal of flexibility regarding inclusion of other control criteria in a SOC 2 report, creating the concept of a SOC 2+ report. Such a report can be used to demonstrate assurance in areas that go beyond the Trust Service categories and address industry-specific regulations and requirements.

Additional "suitable criteria" added to a SOC 2 report must be objective, measurable, complete, relevant, and available.



## SOC 3

- An examination with same underlying scope as a SOC 2, however with the issuance of a "slimmed down" report that is available for general use
- Publicly available for anyone to view
- May be utilized for marketing material
- Includes the independent service auditor opinion, management assertion, and boundaries of the system (no detailed testing matrix)

Framework	SOC 2+ Example
HITRUST (Health Information Trust Alliance)	A 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 controls in their SOC 2 to the HITRUST framework.
NIST (National Institute of Standards and Technology)	A company that maintains governmental contracts for building roads and bridges has contractual obligations to demonstrate how it meets the latest revision of NIST. To demonstrate adherence to the NIST framework, it maps controls in their SOC 2 to NIST 800-53.

# Components of a SOC Report

Report Section No.	Section Name for SOC 1 Report	Section Name for SOC 2 Report
Section 1	<p><b>Independent Service Auditor’s Report</b></p> <p>Independent auditor attestation that expresses an opinion on related subject matter. The possible opinion outcomes are unqualified opinion, qualified opinion, adverse opinion, or disclaimer of opinion.</p>	
Section 2	<p><b>Management’s Assertion</b></p> <p>Written assertion from management that describes the criteria and informs user entities about how the controls are designed and intended to operate to achieve the applicable control objectives or trust services criteria. In addition to being a component of the SOC report, management’s assertion is also included as in appendix within the Management Representation Letter, which is signed by Company executive management and provided to the service auditor.</p>	
Section 3	<p><b>Description of the System</b></p> <p>Management’s description of the system, which incorporates a narrative description of key elements such as an overview of business operations, control environment, systems, controls that achieve control objectives, complementary user entity controls, and complementary subservice organization controls.</p>	<p><b>Description of the System</b></p> <p>Management’s description of the system, which incorporates a narrative description of key elements such as an overview of business operations, control environment, systems, controls that achieve the service commitments and system requirements, based on the trust services criteria, system boundaries, complementary user entity controls, and complementary subservice organization controls.</p>
Section 4	<p><b>Information Provided by Independent Service Auditor Except for Control Objectives and Control Activities</b></p> <p>Testing matrix with control objectives, control activities, tests of operating effectiveness, and exceptions.</p>	<p><b>Information Provided by Independent Service Auditor Except for Trust Services Criteria and Control Activities</b></p> <p>Mapping of trust services criteria to controls, along with a testing matrix that includes control activities, tests of operating effectiveness, and exceptions.</p>
Section 5 (Optional)	<p><b>Other information provided by the service organization</b></p> <p>This optional section is presented by Management to provide additional information not subject to the examination. For example, management’s response to identified exceptions could be added to this section.</p>	

# Typical Path for New SOC report

## SOC Readiness



	1. Define Report Scope	2. Assess Current State	3. Draft Description	4. Remediation	5. SOC Attestation
Objectives	Define the scope relevant to SOC report	Understand current state of controls	Draft initial description	Remediate gaps	Plan and perform SOC attestation
Key Activities	Define the following: <ul style="list-style-type: none"> <li>• Products and services</li> <li>• Business processes*</li> <li>• Control objectives*</li> <li>• System boundaries**</li> <li>• Systems</li> <li>• Locations</li> <li>• Subservice organizations</li> <li>• User entities</li> </ul>	<ul style="list-style-type: none"> <li>• Perform walkthroughs</li> <li>• Map controls to control objectives or TSC</li> <li>• Assess design and implementation of controls</li> <li>• Identify gaps in achieving control objectives or TSC</li> </ul>	Prepare initial draft of the description, including: <ul style="list-style-type: none"> <li>• Principal service commitments and system requirements**</li> <li>• System boundaries**</li> <li>• Control objectives*</li> <li>• Control descriptions</li> <li>• Complementary user entity controls (CUECs)</li> <li>• Complementary subservice organization controls (CSOCs)</li> </ul>	Remediate gaps in achieving control objectives or TSC, which may include: <ul style="list-style-type: none"> <li>• Designing and implementing new controls</li> <li>• Enhancing execution of existing controls</li> <li>• Enhancing documentation as evidence of controls</li> </ul>	<ul style="list-style-type: none"> <li>• Plan attestation considering readiness and remediation status</li> <li>• Determine report type, reporting period, and target issue date</li> <li>• Perform necessary actions for attest service (independence, background checks, etc.)</li> <li>• Develop test plan and perform tests of controls</li> </ul>

Legend

Key activities are typically applicable to all types of SOC reports, unless otherwise noted.

\* Applicable to SOC 1

\*\* Applicable to SOC 2

Note: The service auditor performing the examination can assist and advise the company in readiness activities, however it cannot assume any management roles including remediation.



# SOC Readiness Assessment

**A readiness assessment is a "pre-audit" that provides a basis for understanding control gaps and remediation efforts in preparation for a future SOC attestation. As part of a readiness engagement, Deloitte may advise and assist management in certain readiness activities, such as the following areas:**

- Assist in defining report scope that may be useful to address the needs of user entities
- Advise on potential control objectives that may be useful to user entities for inclusion in a SOC 1 report
- Conduct interviews with control owners and review available documentation to assist management with drafting the control activities and provide feedback on the coverage of control activities to achieve the control objectives or the service commitments and system requirements, based on the trust services criteria
- Advise on the identification of design or implementation control gaps and potential enhancements (new controls, enhanced documentary evidence, modified existing controls, etc.)
- Assist management with drafting portions of the description, such as:
  - Narrative description of control activities that support control objectives or trust services criteria
  - Potential user entity control considerations (i.e., controls that user entities would be expected to have in place)
  - Potential complementary subservice organization controls (i.e., types of controls that subservice organizations would be expected to have in place)



## An additional thought

Identifying and remediating any control gaps prior to embarking upon a formal SOC examination is critical, as the AICPA requires the service auditor to disclose all exceptions once an examination commences, regardless of their magnitude, and depending on their nature, could result in a "qualified" (negative) opinion.

Note: The service auditor performing the examination can assist and advise the company in readiness activities, however it cannot assume any management roles including remediation.

# Your SOC Service Auditor Makes A Difference

## Why Deloitte?



### SOC Leader

Deloitte is a leading provider of SOC services, issuing 800+ SOC reports in the United States annually. Representative clients range from emerging companies embarking on their first SOC report to Fortune 100 companies with many SOC reports.



### Brand Reputation

Deloitte has stood the test of time for more than 100 years. Our reputation is a testament to our commitment to quality and our core values of integrity, objectivity, and technical excellence. Deloitte provides highly effective solutions and brand recognition that promotes trust and confidence.



### AICPA Collaboration

Deloitte has served as an advisor to the AICPA for the past 25+ years. Deloitte participates in AICPA working groups responsible for developing authoritative guidance for emerging areas of assurance. Deloitte recently presented at the 2022 AICPA & CIMA SOC & Third-Party Risk Management Conference.



### Our Practice

We have an extensive team of professionals who specialize in internal controls, risk management, cyber security, ICFR/SOX, and information systems. With over 3,000 Risk & Financial Advisory professionals in the US alone, we have the breadth and depth of qualified resources.



### Audit Quality Leader

Deloitte is a market leader in audit quality, which is backed by a rigorous quality focus and results in leading class assurance. We have demonstrated superior inspection results, with the lowest number of deficiencies in the PCAOB's Part 1 when compared to the other firms.<sup>1</sup>

1. <https://pcaobus.org/oversight/inspections/firm-inspection-reports>

# Let's Talk

## Deloitte & Touche LLP's Third-Party Assurance solution leaders

### **Sara Lademan**

US Third Party Assurance  
Leader  
[slademan@deloitte.com](mailto:slademan@deloitte.com)

### **Shannon Kramer**

Technology  
[skramer@deloitte.com](mailto:skramer@deloitte.com)

### **Katherine Fortune Kaewert**

Technology  
[kfortune@deloitte.com](mailto:kfortune@deloitte.com)

### **Brett Guber**

Insurance  
[bguber@deloitte.com](mailto:bguber@deloitte.com)

### **Chad Phillips**

Life Sciences and  
Healthcare  
[chadphillips@deloitte.com](mailto:chadphillips@deloitte.com)

### **Anthony Fanizza**

Financial Services  
[afanizza@deloitte.com](mailto:afanizza@deloitte.com)

### **Stacie King**

Financial Services  
[stacieking@deloitte.com](mailto:stacieking@deloitte.com)

### **Brandon Bogard**

Energy, Resources, and  
Industrials  
[bbogard@deloitte.com](mailto:bbogard@deloitte.com)

### **Chris Hoff**

Consumer  
[choff@deloitte.com](mailto:choff@deloitte.com)

### **Brandon Brown**

Blockchain and Digital Assets  
[brandonbrown@deloitte.com](mailto:brandonbrown@deloitte.com)

# Deloitte.

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document 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 advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://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.