TOPCERTIFIER
www.topcertifier.com

SERVICE METHODOLOGY FOR SOC Certification

SERVICE ORGANISATION CONTROL

TOPCERTIFIER
www.topcertifier.com

What are SOC Reports?

SOC reports are a way for companies to verify via independent third-party assurance that service providers have appropriate controls in place and are following industry standards before outsourcing a business function to that organization. This gives service providers an opportunity to establish credibility and build trust with customers, investors, business partners, and auditors while gaining a competitive advantage in the marketplace. All SOC examinations are performed as per AICPA guidelines :

During the process of **SOC Implementation** an experienced team of technology consultants and auditors will work closely with your organization's leadership to assure that :

- The final SOC report is tailored to an organization's unique needs thoroughly and timely.
- Business operations and internal control processes are streamlined.
- Contractual obligations and marketplace concerns are met.
- AICPA reporting requirements are met.

How Do I Determine the Type of SOC Report My Business Needs?

There are two primary reasons to undergo for a SOC assessment and certification:

- A customer or prospective customer, or auditor requests a SOC report.
- Your organization decides to proactively earn soc compliance.

In the first scenario, the requester might likely specify the type of SOC report needed. In either scenario, an organization must first consider its goals. Typically, the desired outcome for any organization is to demonstrate its commitment to the appropriate design and effective operation of its internal control environment.

TOPCERTIFIER
www.topcertifier.com

SOC 1, 2, and 3 Comparison Chart

There are 3 distinct types of SOC reports - SOC 1, SOC 2, and SOC 3. Each report varies but provides valuable information that is required to assess the risks and internal controls associated with an outsourced service provider. An independent, third-party auditor is needed to examine and affirm various aspects of an organization before producing the final report.

SOC 1	SOC 2	SOC 3
Report on your internal controls related to financial information or statements.	Report on your internal controls related to five trust services principles: security, availability, integrity, confidentiality and privacy.	Report on the results of SOC 2 in a manner suited to public audience.
Shared mostly to auditors	Shared mostly to customers and stakeholders	Shared to general public
Applicable to companies which process financial information like Medicals Claim Processing, Payroll Services, Lending Companies etc	Applicable to any technology company which is into information processing. Both product as well as service based companies.	Applicable to any public enterprise that has a SOC 2 verified and want to produce a SOC 3 report for larger public audience.

TOPCERTIFIER
www.topcertifier.com

SOC 1 CERTIFICATION

A SOC 1 report focuses on your organization's controls relevant to a user entity's financial reporting. It's a hyper-detailed examination that requires a specialized understanding of the industry and related control environment. The service organization typically specifies its control objectives and related control activities based on the specific services they perform. A SOC 1 report generally includes business process controls involving the completeness and accuracy of transactions, as well as general information technology controls, such as network security and logical access.

Given the limited scope, a SOC 1 report is best suited for organizations that must instill confidence in their controls and safeguards over their customers' financial data. It is often necessary when the user entity is publicly traded and must comply with SOX 404 or similar regulations. Here are some examples:

Recordkeeping Services

Medical claims processing

Payroll Services

Lending services

SOC 2 CERTIFICATION

A SOC 2 report is for service organizations whose user entities do not necessarily rely on controls for financial reporting, allowing providers to meet the needs of a broader range of user entities.

A SOC 2 examination primarily focuses on how data is stored and protected, specifically controls related to the service commitments and system requirements based on the AICPA's trust services criteria (defined below).

- **Security** – Information and systems are protected against unauthorized access, disclosure of information

- **Availability** – Information and systems are available for operation and use to meet 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

SOC 2 Reports can be availed by any technology company which is into information processing. While SOC 1 and SOC 2 reports both have restricted audiences, SOC 2 reports may be given to other parties such as prospective customers, vendor management professionals, regulators, and other key business partners.

SOC 3 CERTIFICATION

Like SOC 2, SOC 3 reports focus on controls relevant to the AICPA's five trust services categories. However, unlike SOC 2, SOC 3 reports are certified and can be made publicly available, making them valuable tools for marketing the effectiveness of your control environment.

Should you desire a SOC 3 report, your organization must first complete a SOC 2, Type 2 examination (more on report types below). SOC 2 and SOC 3 examinations can be performed on one or more of the trust services categories. SOC 3 reports contain much of the same information included in SOC 2 reports, except with a far less detailed description of your controls related to compliance and operations. They also do not include specific control activities, testing procedures, or detailed results over operating effectiveness.

TYPE 1 vs. TYPE 2

All SOC reports (except for SOC 3) can be either Type 1 or Type 2. The difference is primarily based on the period in scope.

- **Type 1 Report** : A TYPE 1 REPORT describes a service organization's suitability of the design and implementation of controls at a specific point in time.

- **Type 2 Report** : A TYPE 2 REPORT ensures that defined control activities are consistently operating effectively over a defined period which is usually 6 months to 1 year time period, thus yielding improved operational performance.

In many instances, a service organization will begin with a Type 1 report to define the control activities, as of a point in time. Once controls are designed and implemented, the Type 2 the report would follow. As the Type 2 report covers a period (i.e., 6 or 12 months) , this report is more valuable to users because it assures that, during a period controls were operating effectively. An organization typically engages an audit firm to complete the Type 2 report, annually.

TOPCERTIFIER
www.topcertifier.com

How Do I Prepare for a SOC Assessment?

When starting your first SOC assessment, it is beneficial to work with your selected third-party a consultant like us to perform an initial gap assessment, allowing you to remediate any gaps before the start of the SOC reporting process. Taking this route helps you to fill the existing gaps in your current system thereby yielding a much more compliant system that is very close to fulfilling the SOC requirements. While each SOC report is different in scope, there are certain areas of focus essential to all SOC assessments. By focusing on the following tasks, an organization can start preparing their employees for a stronger control environment and therefore a more efficient SOC assessment.

DOCUMENTATION

From an auditors' perspective, if it's not documented then it doesn't exist. Although there may be strong internal controls in place, the evidence of occurrence may not be memorialized. Ensure documentation is maintained to support all controls in place (e.g., approval for access grants, employee acknowledgments, maintenance of populations, etc.).

DEFINED POLICIES AND PROCEDURES

To ensure all relevant parties understand their responsibilities to meet organizational objectives, ensure fundamental processes and procedures are documented. This provides a resource for both employees and the auditors to understand the organization's intention within the control environment. The scope of policies should include:

- Organizational procedures to meet contractual obligations
- Means of meeting principal service commitments and system requirements
- Risk management approach

RISK ASSESSMENT

A formalized process facilitated by an annual risk assessment discussion and approved by the board of directors or executive management should exist. In place of a formal annual risk assessment, an organization may also elect to hold quarterly meetings to discuss changes in threats, business operations, etc., and their impact on the overall risk assessment. The risk assessment should include defined risk levels (i.e., low, medium, and high threat) and the Company's remediation approach (i.e., accept, mitigate, or eliminate) with detail as to how the Company has responded or plans to respond in the future.

TOPCERTIFIER
www.topcertifier.com

SOC Implementation Roadmap

While each SOC report has different requirements and objectives, each is generally performed following seven main stages

	PROCESS STAGE	KEY PARTICIPANTS	KEY MATERIALS
1	Scoping	Top Management Auditors, Consiltant	Background on organizational needs and customer requirements
2	Walkthrough and Control Design	Consultant , Process Owners	Existing policies and procedures, materials from time spent with each process owner
3	Gap Assessment	Consultant , Process Owners	Preliminary documentation to support remediation roadmap
4	Remediation	Consultant , Process Owners	Documentation for validation of the control environment
5	Examination Testing	Auditor, Consultant, Process Owners	Process documentation , examination evidence
6	Report	CPA Auditors	Policies and procedures, draft feedback, response to feedback and exceptions
7	Issuance	CPA Auditors	SOC report

Even with first-year examinations, most of the stages can be accomplished within a defined timeline, though the most unpredictable of the stages, is remediation (stage 4).
The level of effort spent on remediation is determined based on the results of the gap assessment (stage 3). During the assessment stage, your audit firm will provide a remediation roadmap to ensure compliance with the applicable SOC criteria. By creating a strong control environment before the start of the examination, you are setting the foundation for an organized, minimally disruptive audit.

TOPCERTIFIER
www.topcertifier.com

SOC Audit Services

Our experienced team advises service organizations on AICPA SOC reporting requirements. We provide valuable information that customers, prospects, and auditors require to assess the risks and internal controls associated with an outsourced service provider.

As a qualified consulting firm in this space, we have had innumerable conversations around education, value, and efficiencies. We take pride in working with organizations that have specific needs, competing priorities, time constraints, and other unique objectives. We understand the value of time, appropriate planning, and education that ensure an examination seamlessly progresses.

About TOPCertifier

TOPCertifier is a globally recognized management consulting firm specialised in information security services and soc assessments.

Headquartered in Bangalore (India), we have operations in over 20 countries with a special focus on the USA, Europe, and Gulf countries. We also have an impressive presence in Asia-Pacific and African regions. We've advised over 2,800 organizations, spanning numerous industries, on accounting, tax, profitability, and business process solutions, since our inception in Jan-2010. With a team of over 200 Industry Expert Consultants, Certified Lead Auditors, and Subject Matter Experts, we have delivered a 100% track record in terms of our certification success rate.

Thank You

TO LEARN MORE,

VISIT WWW.TOPCERTIFIER.COM