Accedere

SOC 1, 2, 3 Reports

Disclaimer

This publication contains general information only and Accedere is not, through this publication, rendering any 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 advisor.

Accedere shall not be responsible for any loss sustained by any person who relies on this publication. As used in this document, “Accedere" means Accedere Inc. Please visit https://accedere.io and email us at info@accedere.io for any specific services that you may be looking for.

Accedere Inc is a Colorado licensed CPA Firm listed with PCAOB. and Cloud Security Alliance as Auditors. Restrictions on specific services may apply.

Table of Contents

01

Introduction

Outsourcing is on the rise despite increasing cyber security & data beaches. In today's challenging world of Blockchain, AI, IoT and Cloud, you need to be a step ahead of your competitors. Think of the SOC Report as your company's "Security Best Practices". You need to demonstrate a level of confidence that your organization can manage your client's most confidential and valuable information, have the procedures and controls in place to provide the required assurance. A SOC Report can provide this assurance for your clients.

> **Rethink your company's cyber security**

Providing an independent third-party assurance such as a SOC report helps address these concerns and helps Service Organizations stay above the competition.

02

Need for SOC Report

A

Regulatory Compliance

Data Security & Privacy are increasing concerns for many organization. this is especially important in cases where data is regulated &/or sensitive as in case of compliance requirements for HIPAA, PCI, GDPR,, CCPA etc. Cloud environments are adding to the complexity of the issue. Privacy laws are being enforced that may lead to heavy fines or penalties.

B

SOX-404 & PCOAB

Under the Sarbanes Oxley Act (SOX) Public companies are required to ensure that proper controls exist at the service organizations for the outsourced services. Public companies have the responsibility to examine the control environment & may be subject to fines and penalties for deficiency of effective Internal Controls over Financial Reporting (ICFR).

C

Vendor Due Diligence

Having a SOC Report is essential for compliance with regulatory requirements. But there's more- Think Beyond Legalities. If you own an organization that sells outsourced services (such as payroll services, data management or cloud services) that can significantly affect the financial health of an user organization, getting a clean SOC Report sends a strong signal to your existing & prospective clients.

D

Data Governance

Data governance issues also relate to regulatory compliance, security, privacy & similar concerns impacting today's organizations. Today's data management & storage landscape, where data entropy & data sprawl are rampant, has wide reaching consequences for data security.

Many companies are storing data in distributed hybrid cloud and even in unmanaged environments thus increasing challenges for regulatory compliance. A data inventory & data flow is often recommended. With increasing IoT devices and data lakes in the cloud, the visibility & control in invariably lost resulting in data sovereignty challenges.

E

Adaptive use of Disruptive Technologies

Disruptive technologies like Blockchain (Distributed Ledger) has emerged as candidate for financial institutions to reform their businesses. The speed & cost of doing business using distributed ledger technology is expected to improve by simplifying back-office operations & lowering the need for human intervention. However, a number of security concerns around this new technology remains a challenge.

> **Change the way you think about the SOC Reports**

03

Examples of organizations that may need SOC Report

04

Specific terms in SOC Reports

User Organization

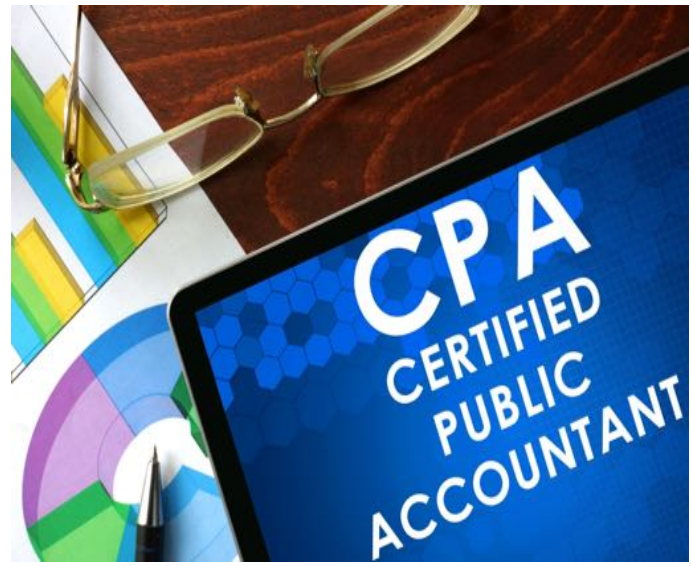
The client/s who requested the report from Service Organization

User Auditor

The client's Auditor that may have demanded the SOC Report

Service Organization

The entity for whose environment the report is being issued

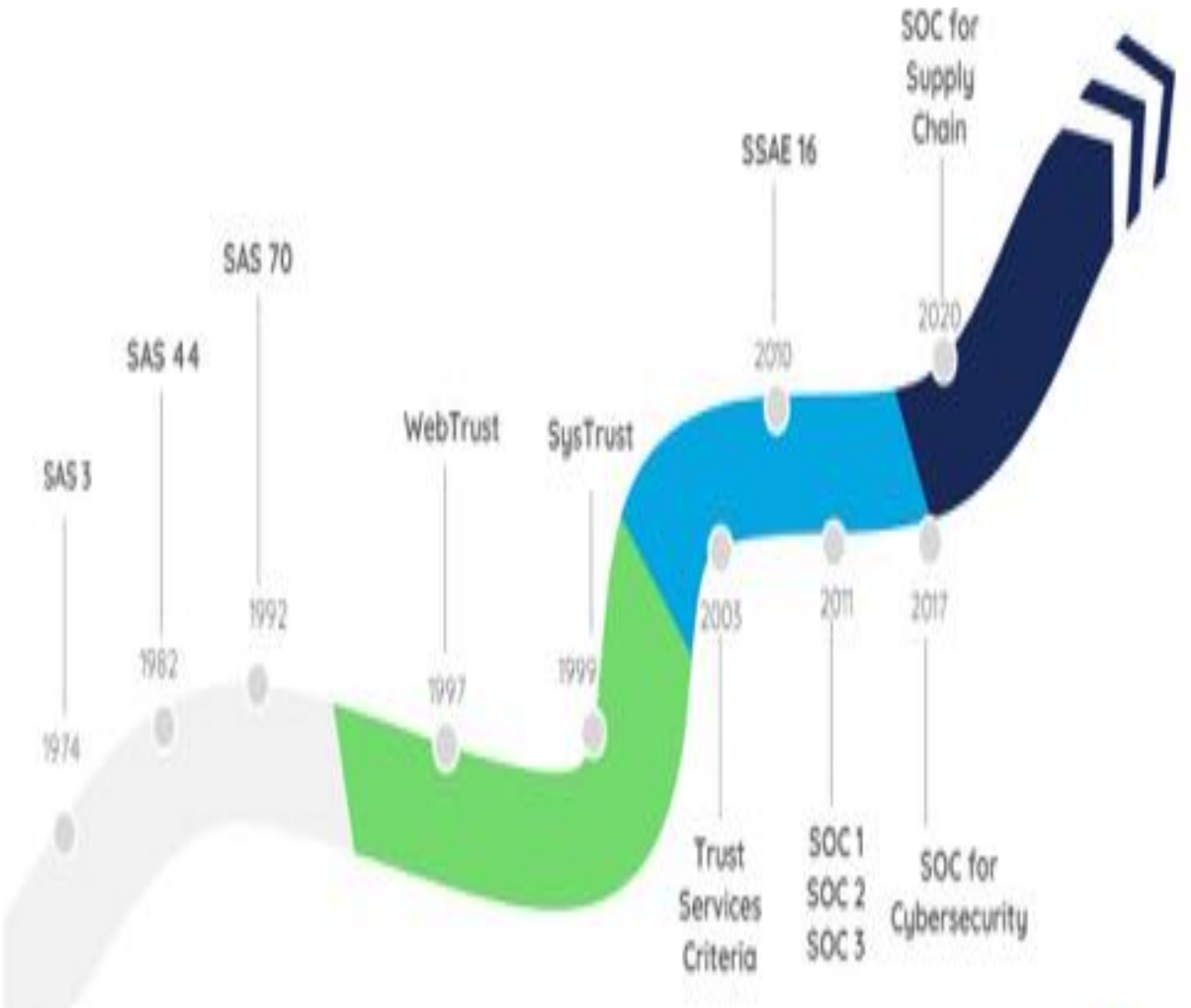


Service Auditor

The CPA Firm that signs the SOC Report

05

SOC Reports History



System & Organizations Controls (SOC)

SOC was formerly known as “Service Organization Controls”. The Service Auditor reports on controls implemented &/or operating effectively at the Service Organization.

The standard requires organizations to demonstrate controls in operations & its design to achieve objectives set forth. SOC report is attested by an Independent Service Auditor. The auditors are subjected to independence training, continuous professional education by the AICPA. Further, the engagements are subject to peer reviews periodically.

SOC uses the SSAE 18 attest standard to evaluate the internal control environment of a service organization.

History of CPA involvement in auditing IT controls

1974	**SAS 3** The effect of EDP on the auditor's study & evaluation of internal control
1982	**SAS 44** Special-purpose reports on internal accounting control at service organizations
1992	**SAS 70** Service Organizations
1997	**Web Trust** Principle & criteria for electronic commerce
1999	**SysTrust** Principles & criteria for system reliability
2003	**Trust Services Criteria (TSC)** For security, availability, process integrity, confidentiality or privacy merger of WebTrust & SysTrust
2010	**SSAE 16** Reporting on controls at a service organization
2011	**SOC 1:** Reporting on Controls at a Service Organization Relevant to User Entity's Internal Control Over Financial Reporting Guide **SOC 2:** Reporting on Controls at a Service Organization Relevant to the TSC Guide **SOC 3:** Trust Services Report for Service Organizations
2017	**SOC for Cybersecurity** Reporting on an entity's cybersecurity risk management program & controls
2020	**SOC for Supply Chain Examination** Reporting on an Examination of Controls Relevant to the TSC in a Production, Manufacturing, or Distribution System

06

Types of SOC Reports

The SOC Engagements can be split into 2 main requirements

SOC 1 or ISAE 3402

Address controls related to user entities Internal Control Over Financial Reporting (ICFR). It is used by service organizations affecting financial reporting of user organization.

Reports are for User Auditor, & Management of User & Service Organization.

SOC 3 Report

A SOC 3 engagement is similar to a SOC 2 engagement. The practitioner (Service Auditor) reports on whether an entity (any entity, not necessarily a service organization) has maintained effective controls over its system with respect to TSC.

A SOC 3 Report may not have details of the controls in the report. It is commonly used in B2C environment.

A SOC 3 report can be shared without an NDA and also displayed on the website .

SOC 2 or ISAE 3000

A SOC Report conveys trust & assurance to users of the system that the service organization has deployed effective control systems, to effectively mitigate operational & compliance risks that the system may represent to its users.

It addresses System & Organization Controls using Trust Services Criteria (TSC) for service organizations to apply and report on controls that may affect users of their service. A SOC 2 Report demonstrates an Independent Auditor's review of a service organization's application of criteria related to one or more of TSC, which are:

Security: The system is protected against unauthorized access.

Availability: the system is available for operations and use as committed or agreed.

Processing Integrity: System processing is complete, accurate, timely and authorized.

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

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

Type 1 & Type 2 Reports

Type I	Type II
Report is as of point in time	Report covers a period of time, generally not less than 6 months & not more than 12 months
Looks at design of controls- not operating effectiveness	Differentiating factor: Includes tests of operating effectiveness
Limited use & considered for information purpose only	May provide the user auditor with a basis for reducing assessment of control risk below maximum
Not considered useful for purpose of reliance by the user auditor	Requires more internal & external effort
Not used as a basis for reducing the assessment of control risk below the maximum	Identifies instances of non-compliance of the stated control activity
Generally performed in the first year that a service organization has a SOC reporting requirement	More emphasis on evidential matter

A Type 2 Report currently provides the most reasonable assurance for the following:

SOC Type II Report can cover the entire year & the effectiveness of the controls in place can be reported.

It is a Third Party Period-of-Time Assessment & so has Accountability.

Since it is a period of time assessment, it is more like a continuous compliance with low risk & high reliability

Most other assurance programs or audits are usually, at appoint in time.

Comprehensive framework for Privacy

Provides a high reliability SOC Seal by AICPA

SOC 1

Purpose:
Audit of Financial Statements

Intended User:
Financial Statements Auditors, Customers, Related Third Parties

Focus On:
Internal controls relevant to Financial Reporting

Type 1:
Design of Internal Control

Type 2:
Design of Internal Control and Operating effectiveness of Internal Control during review period

SOC 2

Purpose:
GRC Programs, Oversight, Due diligence

Intended User:
Management, Regulators, Related Third Parties

Focus On:
Operational controls regarding security, availability, processing integrity, confidentiality or privacy

Type 1:
Design of Internal Control

Type 2:
Design of Internal Control and Operating effectiveness of Internal Control during review period

SOC 3

Purpose:
Marketing or General purpose

Intended User:
Anyone with need for confidence in service organization's controls

Focus On:
Easy to read report on controls

Report Types:
General

Evaluates:
Design of controls related to SOC 2 objectives

07

Typical Statement of Work (SOW)

The SOC reports identifies the standards used by a service auditor to assess the internal controls of a service organization.
The control objectives & criteria vary based on the scope of the SOC report & client operations.

The relationship between the service organization and the user organization must be viewed to help determine the controls that should be included in the engagement.
In addition, the impact on the user organizations financial statements will also be the determining factor as to whether controls at the service organizations are in the scope of the SOC.

The following are some categories for controls activities that are generally included in the Description of Controls for many SOC reviews:

Financial Reporting Controls for SOC 1

In many instances, the financial controls of the service organization affect the financial reporting (ICFR) of the user organization.

Processing Integrity can form an important control objective for SOC 1 engagements.

The financial controls within the organization by use of disruptive technologies such as distributed ledger or blockchain needs to be evaluated.

Trust Services Criteria (TSC) 2017 for SOC 2

This TSC 2017 is effective for all SOC 2 reports signed after December 15, 2018. The 2017 edition revises the TSC to align with the COSO's 2013 Internal Control-Integrated Framework, to better address cybersecurity risks & increase flexibility in application across an entire entity, including at a subsidiary, division, or operating unit level within a function relevant to an entity's operational, reporting, or compliance objectives.

Trust Services Criteria (TSC) 2017 for SOC 2

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 achieve its objectives.

Availability

Information and systems are available for operation and use to meet the entity's objectives. Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers.

Processing integrity

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

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives.

Privacy

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

Although confidentiality applies to various types of sensitive information, privacy applies only to personal information.

The Security category covers about 300 points of focus under the following 9 aspects:

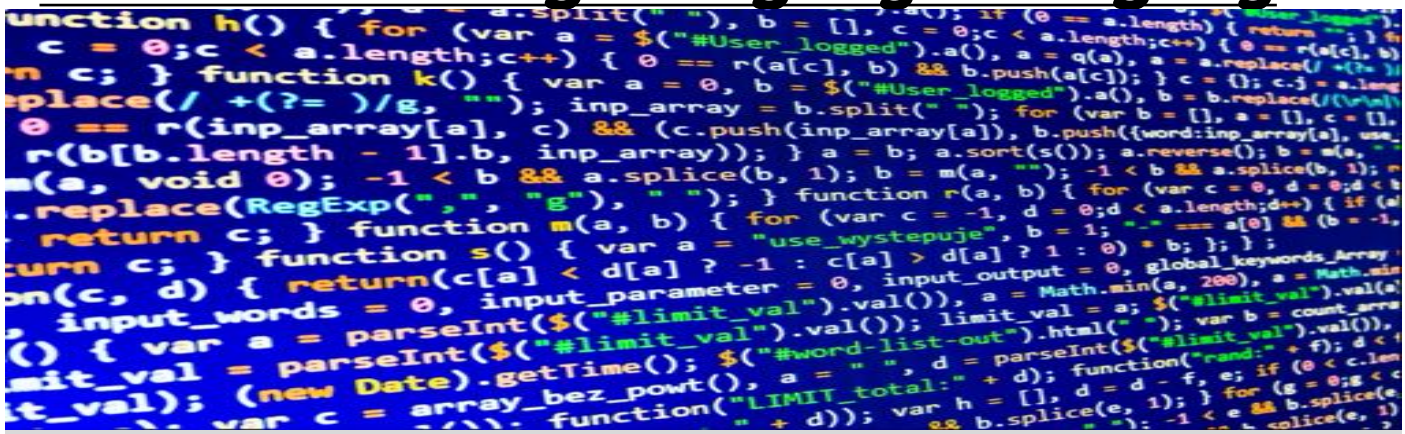
- Control Environment
- Communication & Information
- Risk Assessment
- Monitoring Activities
- Control Activities
- Logical & Physical Access Control
- System Operations
- Change Management
- Risk Mitigation

TSC Availability Category

Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers.

- The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality or usability.
- It addresses whether systems include controls to support accessibility for operation, monitoring, and maintenance.

TSC Processing Integrity Category



Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing.

- Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.
- Processing integrity is usually only addressed at the system or functional level of an entity.

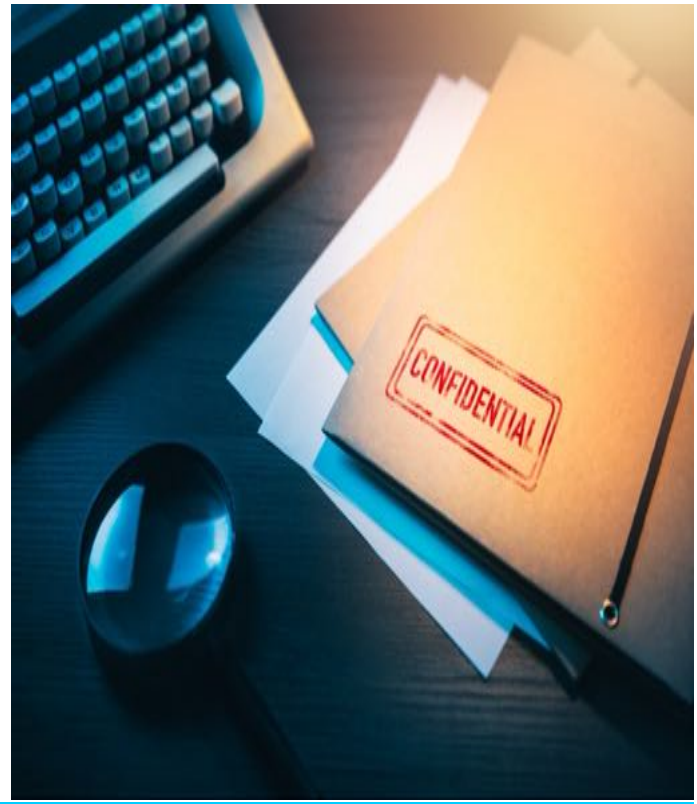
TSC Confidentiality Category

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives.

- Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties.
- Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others.
- The need for information to be confidential may arise as per the contract between parties for many different reasons.

The following points of focus, which apply only to an engagement using the Trust Services Criteria for confidentiality, :

- Identifies Confidential information
- Protects Confidential Information From Destruction
- Identifies Confidential Information for Destruction
- Destroys Confidential Information



Confidentiality v Privacy

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

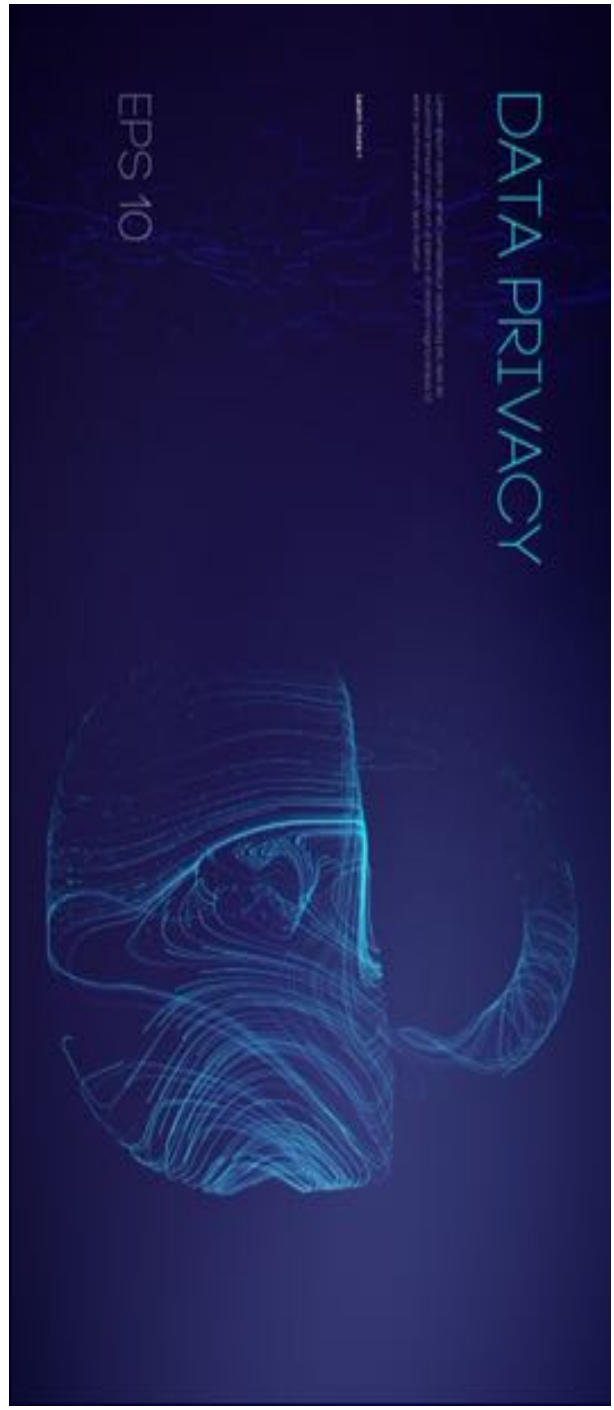
08

TSC Privacy Category

Privacy has become even more important issue in the current environment with several large organizations facing heavy fines.

With about 50 points of focus the TSC 2017 organizes privacy category as under:

- Notice and communication of objectives
- Choice & consent
- Collection
- Use, retention & disposal
- Access
- Disclosure & notification
- Quality
- Monitoring & enforcement



Many of these controls match to the legislations like GDPR, CCPA etc. In the wake of such new privacy mandates organizations are encouraged to include of privacy category in their scope for SOC 2 Report.

09

SOC 2 & COSO Risk Management

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a join initiative of five private-sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence.

In addition to the Trust Services Criteria, the COSO framework, states that the points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy .

Risk Metrics Measurement & Governance

- As per the updated Common Criteria it is important to report on all aspects of risks covering monitoring as well as on effective mitigation. To do an effective monitoring and mitigation, we need to define metrics of measurements where in you define what legal requirements, threats or indicators of compromise you are monitoring and their related controls. Any variance must be monitored daily, weekly or monthly as the case may be and all exceptions or issues must be reported to the Security Governance committee.

- **Create your own security metrics of measurement**
- **Monitor your security metrics on a daily, weekly, monthly basis as the case may be**
- **Report the variance to the risk owner/legal compliance**
- **Report the highlights to your Security Governance Committee**

10

SOC Controls

SOC controls would include the entire commit of People, Process & Technology & how they are used in conjunction to achieve the relevant objectives. The controls would also cover:

Policies

The entity has defined & documented its policies relevant to the particular principle. (The term “policies” as used here refers to written statements that communicate management’s intent, objectives, requirements, responsibilities & standards for a particular subjects.)

Communication

The entity has communicated its defined policies to responsible parties & authorized users of the system.

Procedures

The entity has planned procedures in operation to achieve its principles in accordance with its defined policies.

Monitoring

The entity monitors the system & takes action to maintain compliance with its defined policies.

11

Description Criteria

As part of SOC report a Description of Controls of the system is required from the organization. The new 2017 Description Criteria covers the following areas:

01 **The types of Services Provided**

02 **The Principle Service Commitments & System Requirements**

03 **The Components of the System used to provide the services, including the following:**

- Infrastructure
- Software
- People
- Procedures
- Data

04 **Details of identified System Incidents**

05 **The applicable Trust Services Criteria & related controls**

06 **The controls would be implemented by user entities**

07 **Subservice organizations & the controls at the subservice organization**

08 **Any specific criterion of the applicable Trust Services Criteria that is not relevant**

09 **Relevant details of significant changes to Service Organization's system & controls**

Final Report

- Technically SOC is an Attest report not an Audit report.
- Reports can be either Type I or Type II for controls implemented &/or operating effectively at the service organization.
- It provides information & a service auditors independent opinion about controls at the service organization to its management, stakeholders, and other knowledgeable parties.
- Provides user entities (customers) with detailed information on the design &/or operating effectiveness of service organization's implemented controls.
- Service organizations are required to provide a Management Assertion letter & a System Description which provides the basis of reporting by the service auditor.
- Report can be either as on a specific date or that covers a period, usually 6 or 12 months.

12

New SOC Reports

SOC 2 for Cybersecurity

In 2017, AICPA has developed a cybersecurity reporting framework that organizations can use to demonstrate to key stakeholders the extent & effectiveness of an entity's cybersecurity risk management program. A critical element of any cyber security risk management program is formulation of objectives by management. These objectives that address cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting & operational objectives). Our assessment evaluates the controls in relation to entity's mission & vision, the overall business objectives established by management, risk appetite & other factors.

An examination engagement to report on whether (a) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (b) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

The AICPA and SOC logos are owned by https://www.aicpa.org

SOC for Supply Chain Management

In 2020, recognizing the needs of commercial customers and business partners of manufacturers, producers, and distribution companies, AICPA has developed a framework for reporting on the controls over a manufacturing, production, or distribution system. Organizations can use the reporting framework to communicate to stakeholder's relevant information about their supply chain risk management efforts and the processes and controls they have in place to detect, prevent, and respond to supply chain risks. The reporting framework also enables a CPA to examine and report on management-prepared system information and on the effectiveness of controls within the system, thereby increasing the confidence that stakeholders may place in such information.

An examination engagement to report on whether (a) the description of the entity's system is presented in accordance with the description criteria and (b) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria.

12

SOC 2 Plus Reports

A service organization may engage the service auditor to examine & report on subject matters in addition to the description of the service organization's system in accordance with the description criteria & the suitability of design & operating effectiveness of controls based on the applicable Trust Services Criteria.

SOC 2 for Cloud CSA STAR Attestation

Cloud Security Alliance (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. STAR Attestation provides a framework for CPA's performing independent assessments of cloud providers using SOC 2 engagements with the CSA's Cloud Control Matrix (CCM). Accedere is listed as Auditors with CSA for their STAR Attestation program.

SOC 2 for C5 Cloud Controls

In February 2016, the Bundesamt fur Sicherheit Institute (BSI), or the German Federal Office for Information Security, established the Cloud Computing Compliance Controls Catalog (C5) certification after they noted the rise in cloud computing in the country. With the C5, the BSI redefined the bar that CSP should meet when dealing with German data. The establishment of the C5 elevated the demands on CSP by combining the existing security standards (including international certifications like the ISO 27001) and requiring increased transparency in data processing. C5 is intended primarily for professional cloud service providers, their auditors, and customers of the CSP's. The catalogue is divided into 17 thematic sections (e.g., organization of information security, physical security). C5 makes use of recognized security standards such as 27001, the Cloud Controls Matrix of the Cloud Security Alliance as well as BSI publications and uses these requirements wherever appropriate.

SOC 2 for Privacy

The SOC 2 compliance report assures the internal and external stakeholders of the organization, the specific controls implemented and/or operating effectively for complying with privacy regulatory requirements. A single SOC 2 report can provide information about the organization's controls over PII data based on the AICPA's Privacy Trust Services Criteria and/or any specific privacy requirements. This SOC 2 can provide service organizations the ability to increase transparency and communicate through a single deliverable to customers, business partners, and stakeholders both in and outside the organization. .

cloud CSA security alliance®

CSA STAR™
Security, Trust & Assurance Registry

The CSA , STAR, logos are owned by Cloud Security Alliance

12

Our Project Execution Methodology

Plan	Deliver	Access	Report
Understanding the client's entity & environment	Understanding & verifying documentation of existing internal controls	Evaluate samples	Evaluate additional information
Define scope, expectations & project roles	Perform Walkthrough	Analyse samples for effectiveness	Request clarification
Readiness Assessment if required	Assess Risks	Request additional information	System Description & Management Assertions is drafted through inputs from the audit team by client management
Kick off meeting with Stakeholders	Identifying the control objectives & controls in place		Issue draft report
Preliminary interviews/ questionnaires conducted to gain understanding of requirements	Conduct Interviews		Incorporate Management comments & Issue final report
Client information request list prepared & distributed	Requests Samples		Ongoing support
Analysis of client prepared information performed & client feedback provided	Validation of the implementation of controls		Answer questions to Management & User Auditors
Project timeline (including estimates of client hours) / plan created	Test results communicated & exceptions are resolved, if possible		
Update plan based on client discussions			

Our Value Delivery

Knowing how much extra value and assurance a SOC reports can deliver, many clients find that it makes sense to take steps to ensure a more successful outcome, including hiring experts who are skilled in helping organizations be more thorough and thoughtful in how they approach their engagement. Preparing for a SOC engagement is a matter of clear thinking and smart planning. Working with a cyber security specialist such as Accedere helps you dig into areas such as cloud security, data security, privacy, incident response, and much more.

Some of the advantages of working with us are:

01	End to end process for SOC Reporting & Attest Services
02	Project management methodology consistently applied to each engagement
03	Efficient service delivery with minimal disruption to operations
04	Our engagements are executed by senior experienced professionals
05	CEO has 18 years of Information/ Cyber Security experience
06	Reduced time to complete assignments
07	Colorado licensed CPA Firm listed with PCAOB and Cloud Security Alliance
08	Prompt services with engagements completed in record time
09	Ongoing support
10	We are with you when you need us

For more information visit:

https://accedere.io