Accedere

SSAE 18 & SOC 1, 2, 3 Reports

• • •

INTRODUCTION

Outsourcing is on the rise despite increasing cyber security breaches. 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 handle your clients' most confidential and valuable information, have the procedures and controls in place to provide the required assurance. A SOC report provides this assurance for your clients.

"Rethink Your Company's Cyber Security

NEED FOR SOC REPORT

01

REGULATORY COMPLIANCE

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

02

SOX-404 AND 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 their responsibility to examine the control environment and may be subject to fines or penalties for deficiency of effective **Internal Controls over Financial Reporting (ICFR)**.

03

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 a user organization, getting a clean report of health from a SOC report sends a strong signal of trustworthiness to your existing and prospective clients "**Trust us with yours**."

04

DATA GOVERNANCE

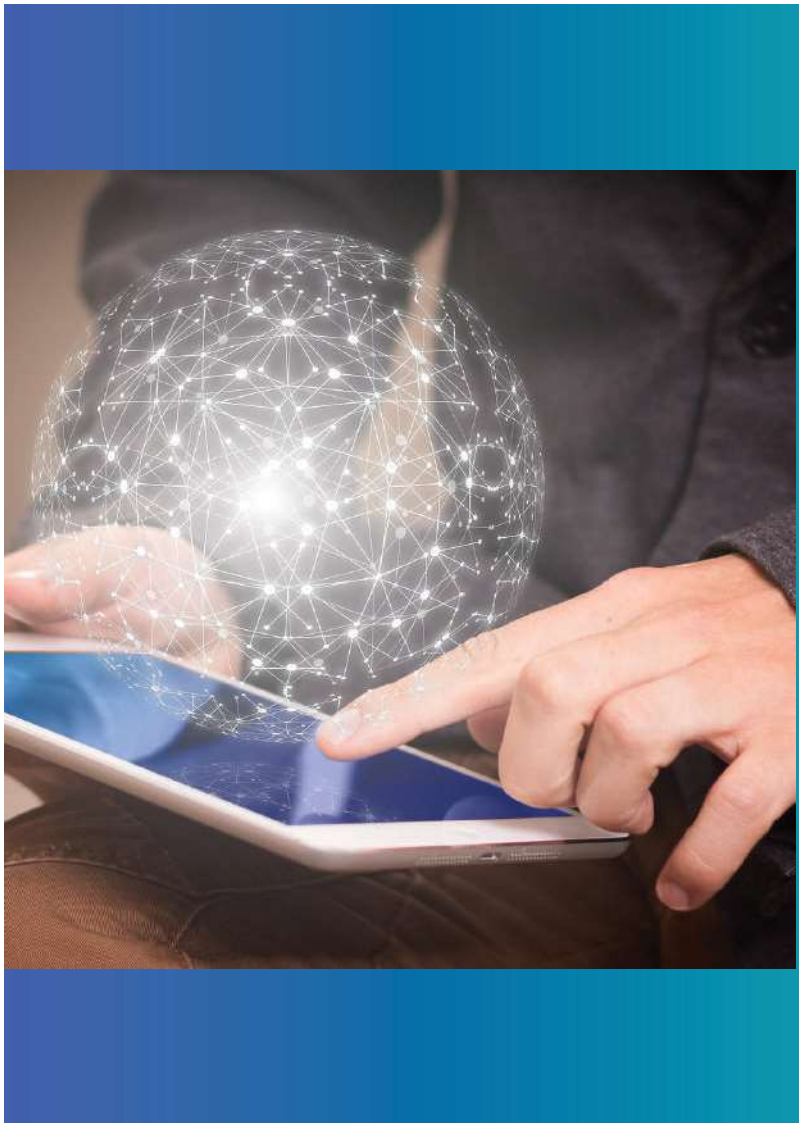
Data Governance issues also relate to regulatory compliance, security, privacy, and similar concerns impacting today's organizations. Today's data management and storage landscape, where data entropy and data sprawl are rampant, has wide-reaching consequences for data security.

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

05

ADAPTING USE OF DISRUPTIVE TECHNOLOGIES

Disruptive technologies like Blockchain (Distributed ledger) has emerged as a candidate for financial institutions to reform their businesses. The speed and cost of doing business using distributed ledger technology is expected to improve by simplifying back-office operations and 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

EXAMPLES OF ORGANIZATIONS THAT MAY NEED A SOC REPORT ARE:

SOFTWARE AS A SERVICE (SaaS) AND APPLICATION SERVICE PROVID-ERS (ASP)

DATA CENTRES/-CO-LOCATION CENTRE'S

HEALTH CARE SERVICES

PAYROLL ORGANIZATIONS

BUSINESS PROCESS OUTSOURCING (BPO) ENTITIES

KNOWLEDGE MANAGEMENT (KM) SYSTEMS

CUSTOMER RELATIONSHIP MANAGEMENT (CRM) SOFTWARE APPLICATIONS

MANAGED SERVICES CENTRE'S

MORTGAGE SERVICE AND PAYMENT ENTITIES

I.T. MANAGED SERVICES ENTITIES

CLOUD SERVICE PROVIDERS

TAFT HARTLEY ORGANIZATIONS

TAX PROCESSING SERVICE PROVIDERS

PAYMENT COLLECTION OR PROCESSING ENTITIES

OTHER FINANCIAL OR INTELLECTUAL PROPERTY SERVICES

SOME SPECIFIC TERMS USED IN SOC REPORT

USER ORGANIZATION

The entity that has engaged a service organization and whose financial statements are being audited.

USER AUDITOR

The auditor who reports on the financial statements of the user organization

SERVICE ORGANIZATION

The entity (or segment of an entity) that provides services to a user organization that are part of the user organization's information system.

SERVICE AUDITOR

The practitioner who reports on controls of a service organization that may be relevant to a user organization's internal control as it relates to an audit of financial statements.

SSAE 18 ATTEST STANDARD & ITS HISTORY*

*Source AICPA

1974
SAS 3
The effects of EDP on the auditor's study and evaluation of internal control

1982
SAS 44
Special-purpose reports on internal accounting control at service organizations

1992
SAS 70
Service organizations

1997
WebTrust
Principle and criteria for electronic commerce

1999
SysTrust
Principles and criteria for system reliability

2003
Trust services criteria (TSC)
For security, availability, process integrity, confidentiality or privacy merger of WebTrust and SysTrust

2010
SSAE 16
Reporting on controls at a service organization

2011
SOC 1®
Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting Guide
SOC 2®
Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy Guide
SOC 3®
Trust Services Report for ServiceOrganizations

2017
SOC for Cybersecurity
Reporting on an entity's cybersecurity risk management program and controls

2018 AND BEYOND: EVOLVE CYBERSECURITY SERVICES AND INTRODUCE SOC FOR VENDOR SUPPLY CHAIN

SYSTEM AND ORGANIZATION CONTROLS (SOC)

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

The standard requires organizations to demonstrate controls in operations and its design to achieve objectives set forth. SOC report is attested by an Independent Service Auditor. The auditors are subjected to independance 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.

TYPES OF SOC REPORTS

THE SOC ENGAGEMENTS CAN BE SPLIT INTO 2 MAIN REQUIREMENTS

SOC 1 OR ISAE3402

Address Controls Related to User Entities' Internal Control over Financial Reporting ("ICFR"). It is used by service organizations affecting financial reporting of user organizations.

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

SOC 2 OR ISAE3000

A SOC 2 report conveys trust and assurance to users of the system that the service organization has deployed an effective control system to effectively mitigate operational and compliance risks that the system may represent to its users.

It addresses System and 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 the TSC, which are:

Security: The system is protected against unauthorized access (both physical and logical).

Availability: The system is available for operation 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 (i.e., information that is about or can be related to an identifiable individual) is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with TSC criteria.

Reports are for Knowledgeable Parties.

SOC 3 REPORT

A SOC 3 engagement is similar to a SOC 2 engagement in that the practitioner 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 environments.

TYPE I AND TYPE II REPORTS

TYPE I	TYPE II
Report is as of point in time (i.e., as of 12/31/200X)	Report covers a period of time, generally not less than 6 months and not more than 12 months
Looks at the design of controls – not operating effectiveness	Differentiating factor: Includes tests of operating effectiveness
Limited use & considered for information purposes only	May provide the user auditor with a basis for reducing assessment of control risk below maximum
Not considered useful for purposes of reliance by user auditors	Requires more internal and external effort
Not used as a basis for reducing the assessment of control risk below the maximum	Identifies instances of noncompliance 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 II REPORT CURRENTLY PROVIDES THE MOST REASONABLE ASSURANCE FOR THE FOLLOWING REASONS:

- SOC Type II report can cover the entire year and the effectiveness of the controls in place can be reported
- It is a Third Party Period- of-Time assessment and so has Accountability
- Since it is a period of time assessment, it is more like a continuous compliance with low risk and high reliability
- Most other assurance programs or audits are usually, at a point in time
- Comprehensive Framework for Privacy
- Provides a high reliability SOC Seal by AICPA

	PURPOSE	INTENDED USERS	FOCUS ON	REPORT TYPE	EVALUATES
SOC1	Audit of Financial Statements	Financial Statement Auditors,Customers, Related third parties	Internal controls relevant to Financial Reporting	Type I	Design of Internal Control
				Type II	Operating effectiveness of Internal Control during review period
SOC2	GRC Programs, Oversight, Due diligence	Management, Regulators, Related third parties	Operational controls regarding security,availability, processing integrity, confidentiality or privacy	Type I	Design of Internal Control
				Type II	Operating effectiveness of Internal Control during review period
SOC3	Marketing or General purpose	Anyone with need for confidence in service organization's controls	Easy to read report on controls	General	Design of controls related to SOC2 objectives

TYPICAL SCOPE 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 and criteria vary based on the scope of the SOC report and client operations.

The relationship between the service organization and the user organizations 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 control 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.

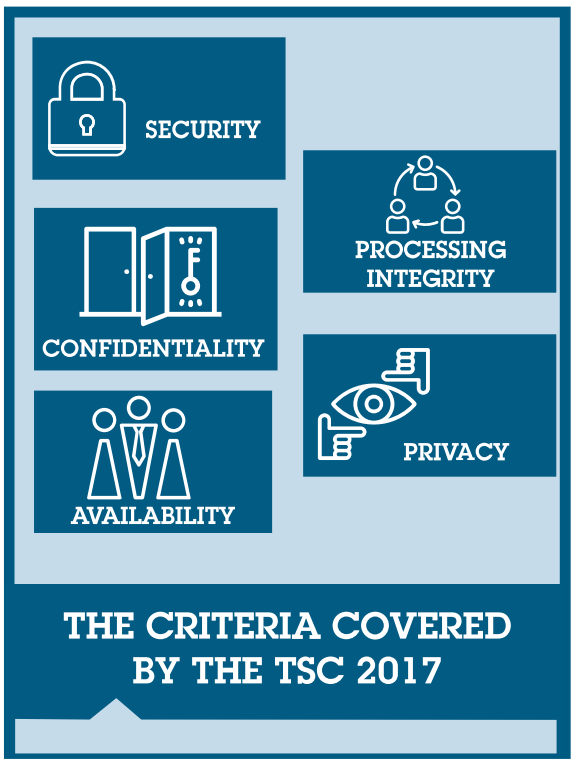
Processing Integrity can form an important control objective for SOC 1 engagements.

The financial controls that should be in scope for the engagement need to be specifically agreed.

Effectiveness of internal 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 Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 2013 Internal Control—Integrated Framework, to better address cybersecurity risks and 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.



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

CONTROL ENVIRONMENT

COMMUNICATION AND INFORMATION

RISK ASSESSMENT

MONITORING ACTIVITIES

CONTROL ACTIVITIES

LOGICAL AND PHYSICAL ACCESS CONTROLS

SYSTEM OPERATIONS

CHANGE MANAGEMENT

RISK MITIGATION

THE PRIVACY CRITERIA

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 criteria as under:

Notice and communication of objectives

Choice and consent.

Collection.

Use, retention, and disposal

Access

Disclosure and notification

Quality

Monitoring and enforcement

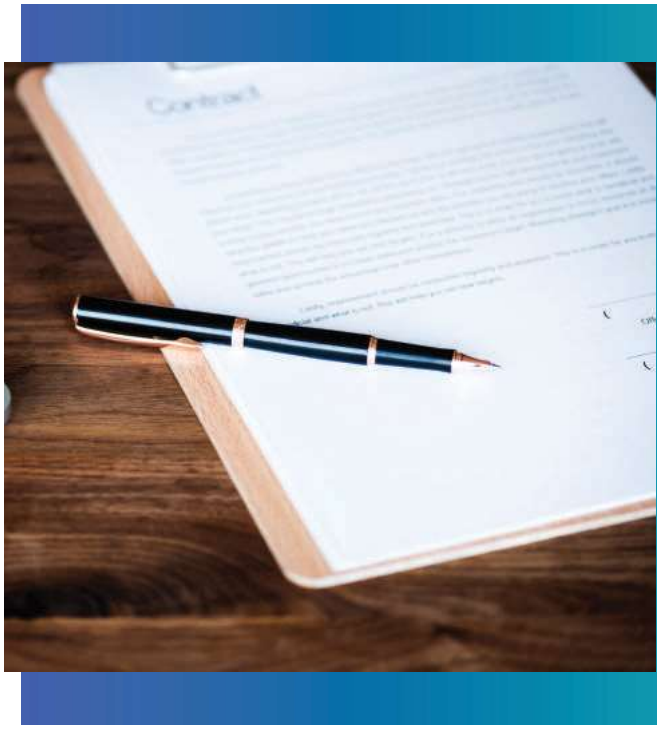
Many of these controls match to the legislations like EU-GDPR. In the wake of such new privacy mandates organizations are encouraged to include of privacy criteria in their scope for SOC 2 report.

SOC CONTROLS

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

POLICIES

The entity has defined and 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 and standards for a particular subject.)



COMMUNICATION

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

PROCEDURES

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

MONITORING

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

DESCRIPTION CRITERIA (DC)

As part of the SOC report is a Description 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 PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

03 THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES, INCLUDING THE FOLLOWING:

a. Infrastructure

b. Software

c. People

d. Procedures

e. Data

04 DETAILS OF IDENTIFIED SYSTEM INCIDENTS

05 THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

06 THE CONTROLS WOULD BE IMPLEMENTED BY USER ENTITIES

07 SUBSERVICE ORGANIZATION AND 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 AND CONTROLS

FINAL REPORTS

» Technically SOC is an Attest Report not an Audit Report.

» Reports can be either a Type I or Type II for controls implemented and/or operating effectively at the service organization.

» It provides information and a service auditors independent opinion about controls at the service organization to itsmanagement, stakeholders and other knowledgeable parties.

» Provides user entities (customers)with detailed information on the design and/or operating effectiveness of the service organization's implemented controls.

» Service organizations are required to provide a Management Assertion letter and a System Description which provides the basis of reporting by the service auditor.

» Report can be either as on a specific date or that coversa period, usually 6 or 12 months.

SOC 2+ ADDITIONAL SUBJECT MATTERS AND ADDITIONAL CRITERIA

A service organization may engage the service auditor to examine and report on subject matters in addition to the description of the service organization's system in accordance with the description criteria and the suitability of design and 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 CPAs performing independent assessments of cloud providers using SOC 2 engagements with the CSA's Cloud Controls Matrix (CCM). We are listed as Auditors with CSA for their STAR Attestation program.

SOC 2 FOR HITRUST

The AICPA HITRUST working group, recently collaborated with HITRUST to develop an SOC 2 report that also incorporates criteria from the HITRUST Common Security Framework (CSF) for performing of SOC 2 plus HITRUST engagements. HITRUST, a health information trust alliance, established the CSF for use by organizations that create, access, store or exchange personal health and financial information. The CSF is an information security framework that incorporates and leverages existing security requirements, including federal (HIPAA, HITECH), third party (PCI, COBIT) and government (NIST, FTC).

SOC FOR CYBERSECURITY

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

OUR PROJECT EXECUTION METHODOLOGY

PLAN	DELIVER	ACCESS	REPORT
Understanding the client entity and environment	Understanding and verifying documentation of existing internal controls	Evaluate Samples	Evaluate additional info
Define scope, expectations and project roles	Perform Walkthrough	Analyse Samples for effectiveness	Request clarifications
Readiness Assessment if required	Assess Risks	Request additional info	System Description and Management Assertions is drafted through inputs from the audit team by the client management
Kick off meeting with Stakeholders	Identifying the control objectives and controls in place		Issue draft report
Preliminary interviews / questionnaires conducted to gain understanding of requirements	Conduct Interviews		Incorporate Management comments and Issue final report
Client information request list prepared and distributed	Request Samples		Ongoing support
Analysis of client-prepared information performed and client feedback provided	Validation of the implementation of controls		Answer questions to Management and User Auditors
Project timeline (including estimates of client hours) / plan created	Test results communicated and 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 ours, 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:

A
- » End to end process for SOC Reporting & Attest Services
- » Project management methodology consistently applied to each engagement

B
- » Efficient service delivery with minimal disruption to operations
- » Our engagements are executed by senior experienced professionals

C
- » 15 years of Information Security & Cyber Security experience
- » Reduced time to complete assignments

D
- » Licensed CPA Firm listed with PCAOB and Cloud Security Alliance
- » Prompt services with engagements completed in record time

E
- » Ongoing support. We are with you whenever you need us

Contact us for a detailed discussion:

Ash (Ashwin Chaudhary)
MBA(IT), CPA, CCSK, CISSP, CISA, CISM, CGEIT, CRISC, PMP,
ac@accedere.us