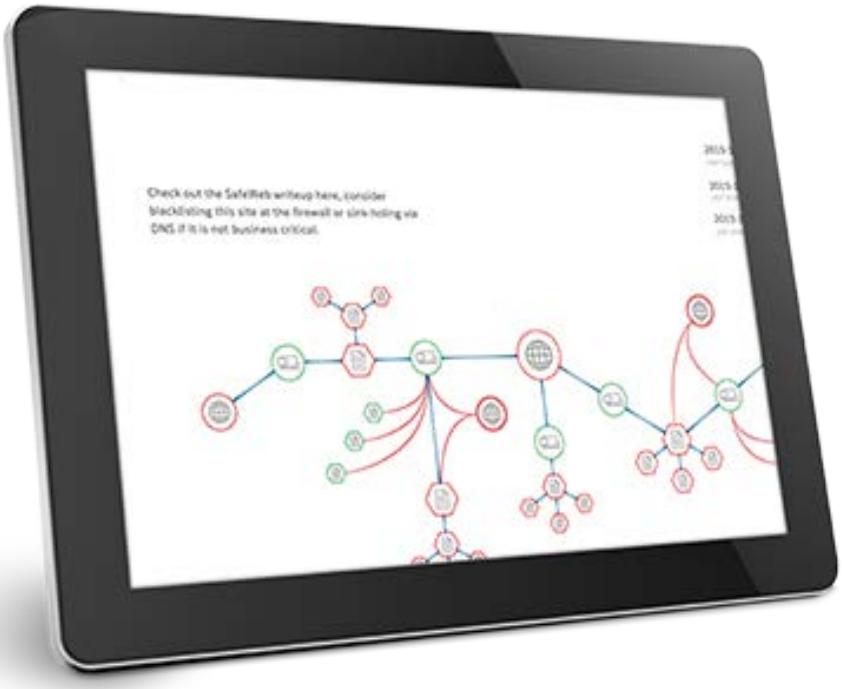


SOC 1 | SOC 2 | SOC 3 Reports

Reinforce confidence of your clients through demonstration of effective controls with an objective report that expresses an opinion about the control environment

You can outsource a process, but you can't outsource the risk...

Introduction

Organizations are increasingly outsourcing systems, business processes, and data processing to service providers in an effort to focus on core competencies, reduce costs, and more quickly deploy new application functionality. As a result, user organizations are updating their processes for monitoring their outsourced vendor relationships, and managing the risks associated with outsourcing. Historically, many organizations have relied upon Statement on Auditing Standards (SAS) 70 reports to gain broad comfort over outsourced activities. However, SAS 70 was intended to focus specifically on risks related to internal control over financial reporting (ICOFR), and not broader objectives such as system availability and security. With the retirement of the SAS 70 report in 2011, a new breed of Service Organization Control (SOC) reports has been defined to replace SAS 70 reports, and more clearly address the assurance needs of the users of outsourced services.

Assurance Reporting

As a service provider there are various ways in which you can provide assurance to your customers and other stakeholders over your control environment. One of the most effective ways is to issue a Service Organisation Control (SOC) Report. The need for this type of assurance reporting can be driven by the following:

- The increasingly regulated corporate environment your customers operate in is forcing them to consider how you demonstrate control effectiveness over the operations they have outsourced to you;
- Slowdown in economic conditions has created a greater need for stakeholders to understand fully, and be confident, with the effectiveness of outsourced processes;
- There is a growing demand in the marketplace for a service organisations to provide a recognised controls assurance report to retain and win business; and
- Accountability for demonstrating management of outsourced risk now extends beyond pure financial risk to assess areas such as Data Security

Introduction to SOC 1, SOC 2, and SOC 3

There are three SOC reporting options currently available in the marketplace – SOC 1, 2 and 3. The SOC reporting options each allow management of a service organisation to provide a level of transparency around their internal controls to their customers and/or perspective customers. To best understand the reporting options it's important to consider the intended use and audience in each case.

The table below provides a side-by-side comparison of the SOC reporting options related to several reporting considerations.

Service Organisation Control (SOC) reports most commonly cover the design and effectiveness of controls for a 12-month period of activity with continuous coverage from year to year to meet user requirements from a financial reporting or governance perspective.

Period of time reports covering design and operating effectiveness are generally referred to as "Type 2" reports whereas point in time reports covering design are generally referred to as "Type 1" reports

	SOC 1	SOC2	SOC 3
Purpose	Report on controls over at service organisation that may be relevant for to user entities' internal controls over financial reporting.	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity	Report on non-financial processing based on one or more of the Trust Service criteria on security, availability, privacy, confidentiality and processing integrity.
Scope	Services and processes covered in the report are defined by the management of the service organisation.	Consists of 1 or more of Trust Service criteria on security, availability, confidentiality, processing integrity and privacy. For each domain principles and controls are predefined.	Services and processes covered in the report are defined by the management of the service organisation
Content	Auditor's Opinion Management Assertion System Description Examination Results Additional Information	Auditor's Opinion Management Assertion System Description Examination Results Additional Information	Auditor's Opinion Management Assertion
Standards	ISAE3402	ISAE 3000	ISAE 3000
	SSAE16	AT 101	AT 101
Types	Type I & Type II	Type I & Type II	Type I & Type II
Audience	Distribution restricted to the users of the services and their auditors.	Distribution restricted to the users of the services, their auditors and specified parties (e.g. prospects).	Distribution to anyone.

The report structure

The following table compares the report components of each SOC option. Generally, a SOC 2 report has a similar 'look and feel' of a traditional SOC 1 report. A SOC 3 report provides a high level summary of information due to its unlimited distribution. Each SOC option can be prepared as a point in time assessment of control design (Type I) or assessment of design and operating effectiveness over a period of time (Type II).

Report components	SOC 1	SOC 2	SOC 3
Auditor's opinion	✓	✓	✓
Management's assertion	✓	✓	✓
Description of the system (including controls)	✓	✓	✓
Control objectives	✓		
Principles and criteria		✓	✓
Auditor's tests of controls	✓	✓	
Auditor's results of testing	✓	✓	
Other information provided by service provider	✓	✓	
Period of coverage	- - - - - - - - **Type I:** Point in time - - - - - - - - - - - - - **Type II:** Minimum of six months - - - - -		

Trust Services Principles and Criteria

SOC 2 and SOC 3 reports use the same framework: the Trust Services Principles and Criteria. There are five Trust Services Principles. The five Trust Principles are:

Principles	
Security	The system is protected against unauthorised access (both logical and physical access), use or modification.
Availability	The system is available for operation and use as committed or agreed. The availability principle refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements.
Processing integrity	System processing is complete, valid, accurate, timely, and authorised.
Confidentiality	Information designated as confidential is protected as committed or agreed.
Privacy	Personal information is collected, used, retained, disclosed and disposed of in conformity with the commitments in the entity's privacy notice and with criteria set forth in the GAPP issued by AICA and CICA (this are expected to be modified in summer 2016).

Each Principle is supported by defined criteria that must be met in order to have a suitably designed system in place. This defined criteria has been updated by the AICPA in December 2014, aiming to increase clarity and reduce redundancy, based on feedback from user entities

and auditors. Many of the criteria applied in the evaluation of a system are shared among all of the principles, for example the criteria relevant to risk management apply to security, availability, processing integrity, confidentiality and privacy principles.

As a result, the criteria for the security, availability, processing integrity, and confidentiality principles are organised into (1) the criteria that are applicable to all four principles (common criteria) and (2) criteria applicable only to a single principle. The common criteria constitute the complete set of criteria for the security principle. For the principles of availability, processing integrity, and confidentiality, a complete set of criteria is comprised of all of the common criteria and all of the criteria applicable to the principle(s) being reported on.

The privacy principle is being revised and reporting on the privacy principle is not currently affected by alignment to the common criteria.

Planning considerations

Before starting a SOC reporting initiative, it's important to plan out a reasonable timeline. We suggest that first-time issuers of a SOC report follow a four-stage approach (see below). Proper scoping and readiness assessments upfront can save significant time and challenges around potential control gaps later on. Early communication between the outsourced service provider and customers will help to set expectations appropriately and help ensure achievement of all parties' objectives and requirements.

Scoping and readiness

- Define scope of services to be covered in report
- Select appropriate SOC reporting option
- For SOC 1 draft control objectives; For SOC 2 or 3 select TSPs for inclusion
- Map existing outsourced service provider controls to the objectives or principles
- Understand and assess the design of controls currently and note gaps

Controls remediation

- Management to remediate control gaps or deficiencies

Type I reporting

- Assess the design of controls at a selected date/point in time
- Develop and assess management assertion
- Develop SOC Type I report, including description of system
- Develop auditor's opinion on design of controls to meet the SOC 1 objectives or SOC 2 or 3 TSPs

Type II reporting

- Assess the design of controls across the period under review
- Test the operating effectiveness of controls across the period under review
- Develop the SOC Type II report, including description of the system
- Obtain and assess the management assertion
- Develop auditor's opinion on the design and operating effectiveness of controls to meet the selected principles

Benefits of service auditor reporting

Third-party attestation reporting provides a range of benefits for users and providers of outsourced services.

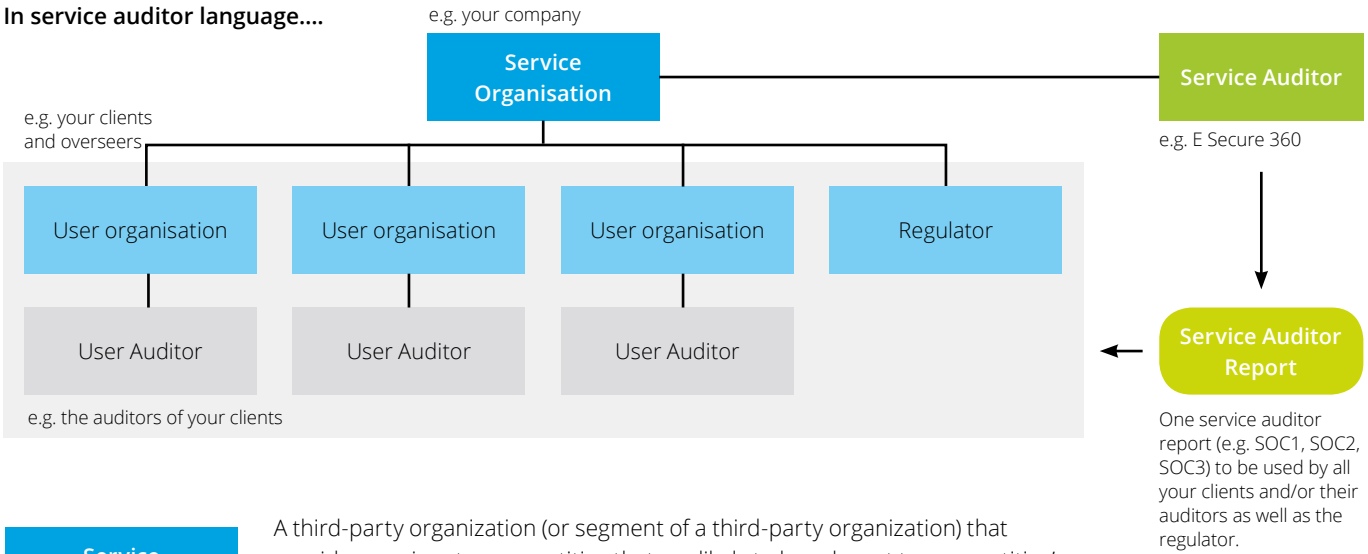
User benefits include

- Ensuring that the expectations of the third-party vendor relationship are met
- Ensuring that the company's multi-purpose reporting requirements — including operational and financial — are met
- Valuable information- independent assessment of whether the controls of the service organization were in place, suitably designed and operating effectively.
- Cost savings- avoiding additional costs in sending the auditors of the user entity to the service organization to perform their procedures.
- Maintaining compliance with industry, governmental and other relevant regulatory requirements.

Provider benefits include

- Commercial advantage – a method to differentiate a service organization from its peers/competitors.
- Cost savings- providing reports issued by the service auditor rather than customer audits – savings on answering questionnaires.
- Broad assurance – provides reasonable assurance to a broad range of clients with a single report.
- Compliance requirements- demonstrates to regulatory bodies that controls are in place and operating effectively.
- Improve overall control awareness- generates increased awareness within the organization of the importance of controls and embeds a strong control culture.

In service auditor language....



Service Organisation — A third-party organization (or segment of a third-party organization) that provides services to user entities that are likely to be relevant to user entities' internal control as it relates to financial reporting.

Service Auditor — A professional accountant in public practice who, at the request of the service organization, provides an assurance report on controls at a service organization e.g. E Secure 360.

User organisation — The entity that has traditionally engaged a service organization to perform services for them that are considered a part of the user organization's "System" e.g. your clients.

User Auditor — The auditor that conducts the financial statement audit on the user organization - these auditors rely heavily on audits from service organizations in helping plan and prepare for the user organization's annual financial statement audit, specifically the auditors of your clients.

How we can help

Our Performance Assurance team is well versed in assisting outsourced service providers and their customers with understanding the SOC reporting options. We can assist organisations through the multi-stage process to issue a Type II SOC report.

Certification granted by the acknowledge industry leader

Our statement on right functioning of your control environment in compliance with SOC standards will increase confidence over matters related to ICFR. We have dedicated experts in risk and controls with a deep industry focus and a wealth of
experience

Clearly structured report

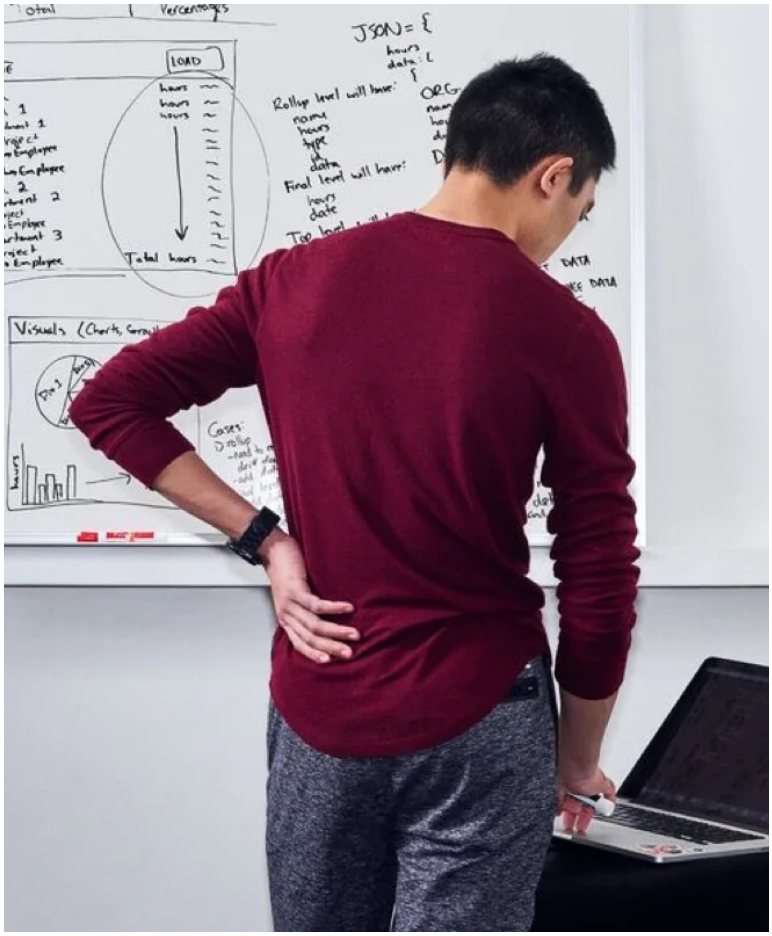
Our output is an easy-to-navigate report adjusted to your organization's specifics. We provide a management summary of
the key issues in which your client will be interested the most.
Naturally, the report is structured by topics so that anything may be searched for and found very fast. All this is provided with respect to the rules and instructions that the report has to meet to be generally acknowledged.

Tested methodology

Our methodology is a functional, effective and practically proven concept, built up on a clear specification of our requirements, continual client communication and validation throughout the engagement. We have our template documents and processes that allow us to effectively manage any part of the project.
A flexible approach together with structured procedures will ensure a seamless course of an audit tailored to your organization's internal processes.

Cost savings

Our SOC reports will avoid additional costs in sending the auditors of the user entity to the service organization to perform their procedures and answering customer questionnaires. Our SOC reports ensure that the expectations of third-party vendor relationships are met and maintaining compliance with industry, governmental, & other relevant regulatory requirements.



Contact us

Douglas Fink
Leader | Risk Advisory
+1.480.530.6007
douglas.fink@esecure360.com

Philip Rushmer
Director | Service Excellence
+44.20.3807.4445
philip.rushmer@esecure360.com

E Secure 360 and its member firms provides cyber security and compliance services to public and private clients spanning multiple industries. E Secure 360, subsidiary of E Com Security Solutions brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges.