# *Building customer trust*

## A perspective on Service Organization Controls reporting options

pwc

www.pwc.com/ca/controls

# Background

Over the past several years, companies have been more aware of the importance of internal controls over third-party hosted systems, services and data. Contributing factors include increasing instances of sophisticated security breaches, disclosure of private and confidential data, and system failures due to disasters impacting service and system reliability, availability, and integrity. In addition, maintaining security and trust, and addressing customers' assurance needs in the increasingly sophisticated cloud computing environments, where on demand network access is provided to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction, have introduced new risks and challenges for organizations.

Further, organizations operating in highly regulated industries are taking a broader focus on risk by developing robust enterprise risk management programs to manage threats. As a result, outsourced service providers are faced with increasing demands to demonstrate their compliance with robust frameworks of internal controls to build customer confidence across a much broader spectrum of risks.

Historically, service providers have defaulted to issuing the former Canadian Institute of Chartered Accountants (CICA) Section 5970 and American Institute of Certified Public Accountants (AICPA) SAS 70 reports as a means to provide customers with broad coverage over their internal controls. With the replacement of Section 5970 and SAS70 in 2011, a new breed of controls reporting options was defined that more clearly seeks to address the expanding assurance needs of customers. Namely, Service Organization Controls (SOC) reports 1, 2 and 3.

This paper provides outsourced service providers and their customers with an understanding of these reporting options, the ability to compare and contrast the options to assist with determining the best fit and suggested steps in scoping and delivering a SOC report.

# *Understanding the options*

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 organization 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. For example, a SOC 1 report is intended to be a communication vehicle between auditors – from the auditor of the outsourced service provider to the auditor of the customer (user organization). Its purpose is to support the financial statement audit of the customer. By contrast, the SOC 2 report is intended to be a communication vehicle to management at the customer organization, including internal audit and compliance management. A SOC 3 report is a vehicle for management at the outsourced service provider to communicate/demonstrate the strength of their internal control posture to any interested parties. The table below provides a side-by-side comparison of the SOC reporting options related to several reporting considerations.

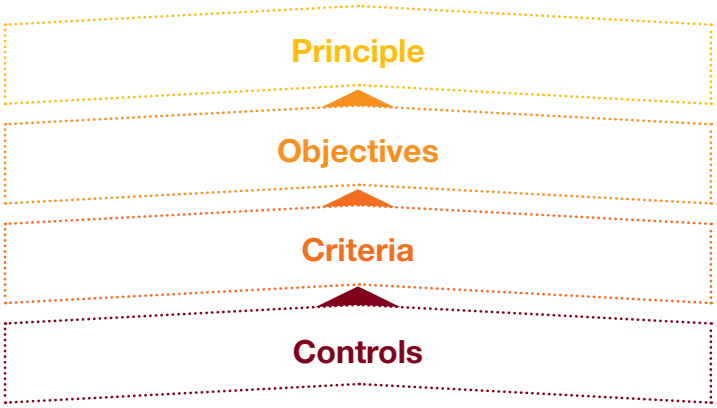
| Considerations | SOC 1 | SOC 2 | SOC 3 |
|---|---|---|---|
| Focus of the engagement | Report on a service organization's controls related to customers financial reporting processes | Report on system reliability using standard principles and criteria | Report on system reliability using standard principles and criteria |
| Are there pre-established control objectives or criteria? | No | Yes: Trust Services Principles | Yes: Trust Services Principles |
| Types of systems addressed by the engagement | Financial systems | Financial and non-financial systems | Financial and non-financial systems |
| Report distribution | Limited | Limited | Unrestricted |
| Intended audience for the report | Service organizations, user organizations, and auditors of the user organizations | Stakeholders of the system—for example, management, customers, and business partners | Any interested parties |

## Understanding the options:
## Taking a closer look at SOC 2 and 3

AICPA and CICA developed the Trust Services Principles (TSP) framework to provide a common framework for systems service providers to benchmark their internal control environment. The TSP framework also provides a means for service providers to demonstrate the effectiveness of their internal controls. The foundation of the TSP framework is a set of five principles (listed below) and criteria that Chartered Accountants (CAs) can use to assess the reliability of an outsourced service provider's systems. A SOC 2 or 3 report can be scoped to include one or more of the TSPs:

- **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 is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set in generally accepted privacy principles (GAPP).

Each TSP is comprised of four objectives: policy, communication, procedure and monitoring. Within each principle and objective, specific criteria are defined related to the areas noted in the table below. Each criterion within a principle must be attained in order to achieve the principle. The TSP framework provides illustrative controls to help outsourced service providers and their customers understand the types of controls that generally satisfy the various criteria. This can be helpful guidance when first undertaking a SOC 2 or SOC 3 reporting initiative. The diagram (below) demonstrates the relationship between the principles, objectives, criteria and control activities in satisfying the principles.




| TSP | Topics covered | |
|---|---|---|
| Security | • Security policies, awareness & communication<br>• Risk assessment<br>• Physical access<br>• Logical access<br>• Security monitoring & compliance | • Problem and incident management<br>• User administration & authentication<br>• Configuration management<br>• Change management |
| Availability | • Availability policies & communication<br>• Data backup & restoration<br>• Data centre environmental controls | • Disaster recovery<br>• Business continuity |
| Confidentiality | • Confidentiality policies, awareness & communication<br>• Confidentiality of data inputs<br>• Confidentiality over data processing | • Disclosures of information (such as third parties)<br>• Confidentiality of data in/during system development efforts |
| Processing Integrity | • Policies over system processing integrity<br>• Completeness of inputs, processing and outputs<br>• Accuracy of inputs, processing and outputs | • Timeliness of inputs, processing and outputs<br>• Validity of inputs processing and outputs<br>• Traceability of data from input to disposition |
| Privacy | • Privacy management<br>• Privacy notice<br>• Consent<br>• Use and retention | • Access to data<br>• Disclosure of data to third parties<br>• Quality<br>• Monitoring and enforcement |

## Understanding the options:
## **Understanding 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 - - - - - - - - <br> - - - - - **Type II:** Minimum of six months - - - - - | | |

# Understanding the options:
# Understanding the benefits

Outsourced service providers and their customers can derive a number of benefits from a SOC report:

- A SOC report allows service provider to build trust with their customer by demonstrating strong internal control practices.
- SOC reporting options provide visibility and transparency to customers around the service provider's operations and internal controls.
- The SOC 2 and 3 reporting options open the door to allow reporting on controls beyond financial reporting, which may result in a streamlined process for receiving and reviewing reports.
- A SOC report demonstrates a strong risk management focus and robust internal controls, which can be an advantage against competitors.
- Since many service providers are global organizations that support clients with international operations, SOC reporting delivers consistent assurance over the security, availability, integrity, confidentiality and privacy of systems and data, and can help measure performance and delivery across similar organizations.
- SOC reporting provides a fresh and independent perspective of risks and controls to both outsourced service providers and their customers.
- SOC reporting provides opportunities to service providers to streamline their internal controls over security, availability, integrity, confidentiality and privacy of systems and data with best practices.

Below is a comparison of the benefits and drawbacks for each SOC option.

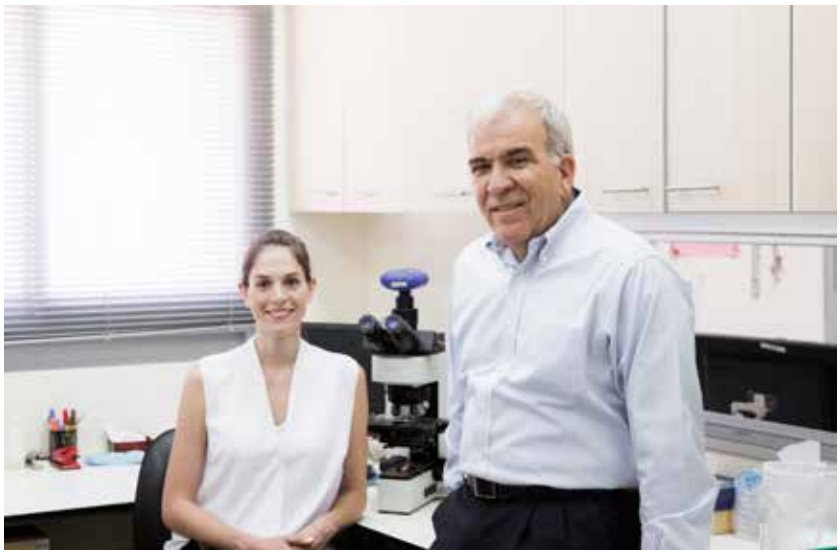
| | SOC 1 | SOC 2 | SOC 3 |
|---|---|---|---|
| **Benefits** | Independent view on outsourced service provider's controls related to customers' financial reporting processes | Scope can be defined to any system | Summary level, easily digested report for customers of outsourced service providers with overall conclusions |
| | Most widely recognized and readily accepted reporting format | Principles and criteria are pre-defined allowing for potential comparison of one provider's controls to another | Unrestricted distribution |
| | Can be relied upon by internal and external auditors | Transparency provided regarding the controls, test procedures and results of testing | Allows the outsourced service provider to include their monitoring controls over aspects of the system supported by a subservice organization |
| | Provides flexibility by allowing subservice organizations to be carved out or included in the scope of the report | Provides flexibility to the outsourced service provider to carve-out subservice organizations | Outsourced service provider may display the SOC 3 seal on its website if all criteria in a principle are achieved |
| **Drawbacks** | Scope limited to systems and processes related to financial reporting of customers | If a subservice organization is carved out, then the customer may need additional reports to gain comfort over those aspects of the system/service | Doesn't allow for carving out significant subservice organizations involved in delivery of the service |
| | Since control objectives are specified by the outsourced service provider, it's often difficult to compare one provider's report to another | Distribution limited to current and perspective customers of the outsourced service provider's service(s) in scope | If one or more criteria in a principle aren't met, then the principle is not achieved (and the seal cannot be displayed) |
| | Distribution limited to current customers of the outsourced service provider's service(s) in scope | Outsourced service providers may be hesitant to share details of their controls, tests performed and results for concern of disclosing sensitive information | Doesn't provide details regarding the controls, test procedures and results of testing at the outsourced service provider |

# *Choosing the best fit* Key considerations

Since the SOC reporting options were first introduced, there's been significant discussion around what types of services and what types of controls are best suited for reporting under SOC 1 versus SOC 2 and/or SOC 3. For some organizations, the answer may be to issue more than one report to fully satisfy their customers' needs and requirements. For a number of organizations issuing a SOC 2 report, they also issue a SOC 3 report to take advantage of the unrestricted distribution characteristic of this report.

The main challenge that many organizations face in determining which reporting option to use often lies in the type of request. A SOC 1 report is often requested but this only covers financial risks and not operational risks therefore organizations need to focus on who will be the users of the report and what risks they need transparency around. When determining which SOC report(s) are the best fit to issue (as the outsourced service provider) or request (as the customer and report user), the following questions are important to consider:

- Does the system impact the financial reporting processes of customer(s)?
- Is there a need for transparency around risks related to technical security, availability, confidentiality and/or privacy?
- Is there a subservice organization involved in delivery of the system/service? If so, is there a requirement to cover their controls in the reporting?
- Is the service provided via a public or hybrid cloud model (i.e. software-as-a-service, infrastructure-as-a-service, platform-as-a-service)?
- Is there a competitive advantage that can be derived by the outsourced service provider by issuing one or more of these reports?



## Choosing the best fit:
## Applying the SOC options

When considering the broad spectrum of services provided by outsourced service providers in today's marketplace, some service types lend themselves clearly to one SOC reporting option over another. For example, traditional payroll processing, claims management, and payment processing lend themselves to SOC 1 reporting due to their direct relationship with customers' financial reporting processes. Meanwhile, there are a number of emerging services (such as cloud services) that tend to lend themselves to SOC 2 and/or 3 reporting. Additionally, there are services that don't clearly align to just one type of SOC report – in these cases the outsourced service provider should work with their customers to clearly define and understand their requirements and select the most suitable fit.

| SOC1 reporting | Case-by-case selection of reporting | SOC 2/3 reporting |
|---|---|---|
| Financial services/asset management | Data centre collocation | Software-as-a-service (SaaS) systems housing third-party data |
| Claims processing | IT systems management | Cloud email services |
| Payment processing | Infrastructure and platform as a service for financial reporting related systems | Cloud HR services |
| Payroll processing | | Other services where security, availability, confidentiality and privacy are risks |

# *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

# 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 organizations through the multi-stage process to issue a Type II SOC report.

**Specifically, our team can help you with:**

### 1. Defining benefits and scope

- Evaluate service offerings and determine the suitability of each SOC reporting option, including benefits and potential drawbacks.
- Assist management to define the scope of the report.
- Help management define a plan to transition or augment their existing reporting.

### 2. Conducting a readiness assessment

- Assist outsourced service provider management with identifying and mapping existing controls.
- Assess the current design controls and perform operating effectiveness testing to highlight areas where controls could improve.
- Identify design/operating effectiveness gaps and provide recommendations to management for consideration and remediation prior to the actual SOC report.

### 3. Preparing the SOC report(s)

- Develop system descriptions for the SOC report(s).
- Guide the development of a management assertion and risk assessment process.
- Define and execute tests of controls for design and/or operating effectiveness (depending upon whether a Type I or Type II report is being delivered).
- Draft and issue SOC report, including auditor's opinion.
- Assist obtaining SOC seals for the outsourced service provider's website.

### 4. Enhancing customer vendor management guidelines

- Reassess vendor management guidelines for outsourced service providers.
- Provide guidance in leading practices for effectively leveraging the SOC reporting options.
- Assist management with developing a framework for reviewing and relying upon SOC reports from their outsourced service providers.

# *Who to call*

## Calgary/ Edmonton

**Justin Abel**
403 509 7522
justin.abel@ca.pwc.com

## Montreal

**Marc Fournier**
514 205 5201
marc.fournier@ca.pwc.com

## Ottawa

**Anthony Dias**
613 755 5945
anthony.j.dias@ca.pwc.com

## Toronto

**Peter Hargitai**
416 941 8464
peter.hargitai@ca.pwc.com

**Jennifer Johnson**
416 947 8966
j.a.johnson@ca.pwc.com

**Jaideep Khatau**
416 814 5846
jaideep.k.khatau@ca.pwc.com

**Tony Pedari**
416 941 8226
tony.pedari@ca.pwc.com

**Kenneth Stoneham**
416 814 5807
kenneth.m.stoneham@ca.pwc.com

## Vancouver

**Kartik Kannan**
604 806 7082
kartik.kannan@ca.pwc.com

## Winnipeg

**Robert Reimer**
204 926 2442
robert.j.reimer@ca.pwc.com

www.pwc.com/ca/controls