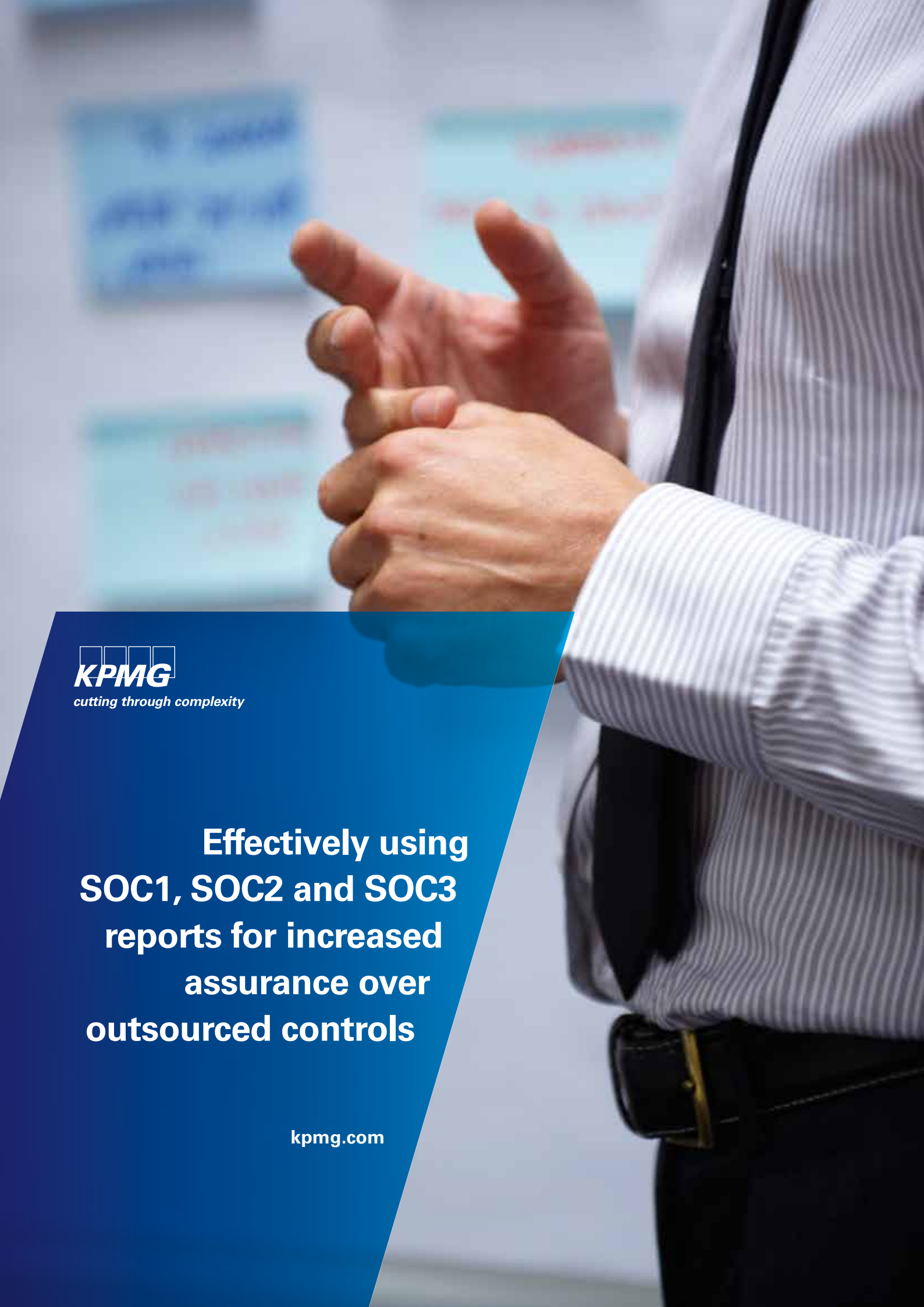

KPMG
cutting through complexity

Effectively using SOC1, SOC2 and SOC3 reports for increased assurance over outsourced controls

kpmg.com

Introduction

Organisations 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, organisations are updating their processes for monitoring their outsourced vendor relationships and managing the risks associated with outsourcing. Historically, many organisations have relied upon 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, the American and Canadian Institutes of Chartered Accountants developed a new breed of Service Organisation Control (SOC) reports which more clearly address the specific assurance needs of the users of outsourced services.

Service Organisation Control or 'SOC' reports refer to ISAE 3402, SSAE16 (or SOC1) and SOC2/3 reports. SSAE16 reports were branded as SOC1 reports by the AICPA (American Institute of Certified Public Accountants), and this is now commonly accepted nomenclature for both reports globally. The AICPA is viewed as the global leader in Service Organisation Control reporting, from their establishment of the SAS70 standard through to current day standards. Outside the US and Canada the SOC2/SOC3 report principles and criteria can be used as a framework for assurance reports under the general ISAE 3000 standard.

This paper provides user organisations (customers) and service providers an overview of SOC2/SOC3 and guidance for the application of SOC2/SOC3 reporting, including the following topics:

Overview of SOC2/SOC3 Reporting

- SOC reporting options
- SOC report types
- Contrasting the scope of SOC2/SOC3 and ISAE 3402/SOC1 reports
- SOC2/SOC3 principles
- SOC2/SOC3 criteria
- Applicability to different types of outsourced services
- Contrasting the level of detail provided by SOC2 and SOC3 reports
- SOC reports structure

Application of SOC2/SOC3 Reporting

- Applicability to different types of outsourced services
- Leading practices for user adoption of SOC2/SOC3
- Key considerations when evaluating assurance reports
- Leading practices for service provider adoption of SOC2/SOC3
- Point of view on the use of SOC reports

Overview of SOC2/SOC3 Reporting

SOC reporting options

SOC refers to Service Organisation Control reports in general, ISAE 3402/SOC1 and SOC2/3.

In the past, the SAS 70 report was intended to assist service organisations' users and their auditors in the context of a financial statement audit. Now, three types of SOC reports (summarised below) have been defined by the AICPA to replace SAS 70 and address a broader set of specific user needs – such as addressing IT security, privacy, and availability concerns. The replacement of SAS 70 by SOC1 in the US and Canada has been based on the international ISAE 3402 standard.

	Internal Control Over Financial Reporting (ICOFR)	Operational controls	
	ISAE 3402/SOC1*	SOC2	SOC3**
Summary	Detailed report for users and their auditors	Detailed report for users, their auditors***, and specified parties	Short report that can be more generally distributed, with the option of displaying a web site seal
Applicability	• Focused on financial reporting risks and controls specified by the service provider. Most applicable when the service provider performs financial transaction processing or supports transaction processing systems.	• Focused on: – Security – Availability – Confidentiality – Processing Integrity and/or – Privacy. • Applicable to a broad variety of systems	

* *Sometimes also referred to as SOC1, SSAE16, AT101 or ISAE 3402 report*

** *Sometimes also referred to as a SysTrust, WebTrust or Trust Services report*

*** *Based on the ISAE 3402 audit standard these reports can, after the evaluation of suitability of the criteria by the user auditor, be useful for the financial audit of the user entity.*

SOC report types

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. In some cases, a SOC report may cover a shorter period of time, such as 6 months, if the system/service has not been in operation for a full year or if annual reporting is insufficient to meet user needs. A SOC report may also cover only the design of controls at a specified point in time for a new system/service or for the initial examination (audit) of a system/service.

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. For example, if a user organisation required a period of time report covering Security and Availability for a particular system, the user organisation would request a SOC2 Type 2 Security and Availability report from the service provider. If the user organisation required a period of time report covering financial reporting (ICOFR) related controls for a particular system, the user organisation would request an ISAE 3402/SOC1 Type 2 report of that system from the service provider.

Contrasting the scope of SOC2/SOC3 versus ISAE 3402/SOC1 reports

The table below compares and contrasts the required focus, scope and control domains covered by SOC2/SOC3 versus ISAE 3402/SOC1 reports.

	ISAE 3402/SOC1	SOC2/SOC3
Required focus	Internal control over financial reporting	Operational controls
Defined scope of system	• Classes of transactions • Procedures for processing and reporting transactions • Accounting records of the system • Handling of significant events and conditions other than transactions • Report preparation for users • Other aspects relevant to processing and reporting user transactions	• Infrastructure • Software • Procedures • People • Data
Control Domains Covered	• Transaction processing controls* • Supporting IT general controls *Note: In certain cases, a report might cover supporting IT controls only, depending on the nature of services provided.	• Security • Availability • Confidentiality • Processing Integrity and/or • Privacy
Level of Standardisation	• Control objectives are defined by the service provider and may vary depending on the type of service provided.	• Principles are selected by the service provider. • Specific pre-defined criteria are used rather than control objectives.

SOC2/SOC3 Principles

SOC2 and SOC3 reports use the globally recognised Trust Services Principles and Criteria, a set of specific requirements developed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) to provide assurance beyond internal controls over financial processes. Principles and Criteria are specifically defined for Security, Availability, Confidentiality, Processing Integrity and Privacy (see the table over the page). This has been done in a modular way so that a SOC2 or SOC3 report could cover one or more of the principles depending on the needs of the service provider and its users.

In contrast, ISAE 3402/SOC1 reports require a service organisation to describe its system and define its control objectives and controls that are relevant to users' internal control over financial reporting. An ISAE 3402/SOC1 report generally should not cover services or control domains that are not relevant to users from a financial audit (ICOFR) perspective and it specifically cannot cover topics such as disaster recovery and privacy.

Criteria	Trust Services Principle	Applicability
Security	• The system is protected against unauthorised access (both physical and logical).	• Most commonly requested area of coverage. • Security criteria are also incorporated into the other principles because security controls provide a foundation for the other domains. • Applicable to all outsourced environments, particularly where enterprise users require assurance regarding the service provider's security controls for any system, non-financial or financial.
Availability	• The system is available for operation and use as committed or agreed.	• Second most commonly requested area of coverage, particularly where disaster recovery is provided as part of the standard service offering. • Most applicable where enterprise users require assurance regarding processes to achieve system availability SLAs as well as disaster recovery which cannot be covered as part of ISAE 3402/SOC1 reports*.
Confidentiality	• Information designated as confidential is protected as committed or agreed.	• Most applicable where the user requires additional assurance regarding the service providers practices for protecting sensitive business information.
Processing Integrity	• System processing is complete, accurate, timely, and authorised.	• Potentially applicable for a wide variety of non-financial and financial scenarios wherever assurance is required as to the completeness, accuracy, timeliness and authorisation of system processing.
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 forth in globally recognised privacy principles (GAPP) issued by the AICPA and CICA.	• Most applicable where the service provider interacts directly with end users and gathers their personal information. • Provides a strong mechanism for demonstrating the effectiveness of controls for a privacy program.

** Depending on national financial audit regulations back up and recovery controls can be in scope of an ISAE 3402/SOC1 report under local regulations.*

SOC2/SOC3 criteria

For most first time SOC2 reports, starting with the Security Principle is often the most practical approach. As mentioned above, Security is the most common area of user focus and the Security criteria in large part form the foundation for the other Trust Services Principles. In addition, the Security criteria are relatively consistent with the requirements of other security frameworks such as ISO 27001. If the organisation already has a security program based on a standard such as ISO 27001 or if they historically completed a SAS 70 examination that covered IT controls at a detailed level, many of the Security criteria topics may already be addressed.

Security

- IT security policy
- Security awareness and communication
- Risk assessment
- Logical access
- Physical access
- Security monitoring
- User authentication
- Incident management
- Asset classification and management
- Systems development and maintenance
- Personnel security
- Configuration management
- Change management
- Monitoring and compliance

Building upon Security, Availability is also a frequent area of enterprise user focus given increasing business dependencies on the availability of outsourced systems and the desire for assurance regarding system availability SLAs. The table below summarises the topics covered by the Security and Availability Principles and Criteria.

Availability

- Availability policy
- Backup and restoration
- Environmental controls
- Disaster recovery
- Business continuity management

Principles and Criteria are also established for Confidentiality, Processing Integrity and Privacy with the covered topics summarised below. Whereas the Security criteria provide assurance regarding the service provider's security controls, the Confidentiality criteria can be used to provide additional detail regarding processes specifically for protecting confidential information.

Confidentiality

- Confidentiality policy
- Confidentiality of inputs
- Confidentiality of data processing
- Confidentiality of outputs
- Information disclosures (including third parties)
- Confidentiality of Information in systems development

The Processing Integrity Criteria can be used to provide assurance regarding a wide range of system processing beyond processing that would be relevant to users from purely an ICOFR perspective and where users cannot gain such assurance through other means, such as monitoring processes.

Processing Integrity

- System processing integrity policies
- Completeness, accuracy, timeliness, and authorisation of inputs, system processing, and outputs
- Information tracing from source to disposition

The Privacy Criteria can be used to provide assurance regarding the effectiveness of a privacy program's controls. We note however that this can be a complex area for organisations with multiple service offerings and geographically diverse users. Even more so than with the other criteria areas, significant preparation is typically required before completing a SOC2 report including the Privacy Principle.

Privacy

- Management
- Notice
- Choice and consent
- Collection
- Use and retention
- Access
- Disclosure to third parties
- Quality
- Monitoring and enforcement

Contrasting the level of detail provided by SOC2 and SOC3 reports

As discussed earlier, SOC2 and SOC3 reporting both use the Trust Services Principles and Criteria and the auditor's work is substantially the same. Having determined which Principles are most relevant to its users, a service provider will need to determine whether detailed SOC2 reporting or summary level SOC3 reporting will satisfy the needs of its users. In both cases, a detailed examination is performed based on the specific criteria; however, the SOC2 report includes detailed information on the service provider's controls and the auditors' individual test procedures and results. Where as the SOC3 report is a more summarised report.

	SOC2	SOC3
Common benefits	• Detailed examination based on defined criteria for Security, Availability, Confidentiality, Processing Integrity, and/or Privacy • Report includes a brief system description • Report includes management's assertion regarding controls	• Where subservice providers are used, management may include its monitoring controls over of those operations
Unique benefits	• SOC2 is more flexible than SOC3 for the service provider in that it permits carveout of supporting services provided by subservice providers. • SOC2 includes detail on the service provider's controls as well as the auditor's detailed test procedures and test results, enabling the reader of the report to assess the service provider at a more granular level.	• SOC3 provides an overall conclusion on whether the service provider achieved the stated Trust Services criteria and the user does not need to digest pages of detailed control descriptions and test procedures. • If the service provider meets all of the criteria, they may choose to display the SOC3 Seal on their website which links to the SOC3 report.
Potential drawbacks	• The user may need to obtain additional reports from significant subservice providers to gain comfort over their activities. • The user may not want to review the detail of the report (controls, tests, etc.) rather than an overall conclusion. • Service providers may not be willing to share a detailed report due to concerns regarding disclosing sensitive information (i.e. detailed security controls).	• SOC3 does not permit carve out of significant subservice provider activities. If it is not feasible to cover those activities as part of the service provider's audit, SOC3 is not an available option. • If one or more of the criteria are not met, the service provider would not be able to display the SOC3 seal until the issue(s) are corrected and re-audited.

SOC report structure

The following table compares and contrasts the structure and contents of SAS 70 and Service Organisation Control (SOC) reports and gives an illustration of the output of the report. Each of these reports can cover a point in time (design -Type 1) or period of time (design and operating effectiveness -Type 2).

The following is a representative comparison of the detailed sections of the reports.

Traditional SAS 70	ISAE 3402/SOC1	SOC2	SOC3
Auditor's Opinion	Auditor's Opinion	Auditor's Opinion	Auditor's Opinion
–	Management Assertion	Management Assertion	Management Assertion
System Description (including controls)	System Description (including controls)	System Description (including controls)	System Description (including controls)
Control objectives	Control objectives	Criteria	Criteria (referenced)
Control activities	Control activities	Control activities	–
Tests of operating effectiveness*	Tests of operating effectiveness*	Tests of operating effectiveness*	–
Results of tests*	Results of tests*	Results of tests*	–
Other Information (if applicable)	Other Information (if applicable)	Other Information (if applicable)	–

* Note: Applicable for Type 2 reports

Traditional SAS 70 and ISAE 3402/SOC1

Control Objective 1: XXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	• • XXXXXX • • XXXXXX	XXXXX
XXXXX	• • XXXXXX • • XXXXXX	XXXXX
–	• • –	–

Control Objective 2: XXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	• • XXXXXX • • XXXXXX	XXXXX
XXXXX	• • XXXXXX • • XXXXXX	XXXXX
–	• • –	–

Control Objective X: XXXXXXXX

Control	Test Procedures	Results of Tests
XXXXX	• • XXXXXX • • XXXXXX	XXXXX
XXXXX	• • XXXXXX • • XXXXXX	XXXXX
–	• • –	–

SOC2

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

1.0 Policies: The entity defines and documents its policies for the security of its system.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• • XXXXXX • • XXXXXX	XXXXX
–	• –	• • –	–

2.0 Communications: The entity communicates its defined system security polices to responsible parties and authorised users.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• • XXXXXX • • XXXXXX	XXXXX
–	• –	• • –	–

3.0 Procedures: The entity uses procedures to achieve its documented system security objectives in accordance with its defined policies.

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• • XXXXXX • • XXXXXX	XXXXX
–	• –	• • –	–

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

Criteria	Control	Test Procedures	Results of Tests
XXXXX	XXXXX	• • XXXXXX • • XXXXXX	XXXXX

Application of SOC2/SOC3 Reporting

SOC 1 financial reporting controls

- Financial services – Custodial services
- Healthcare claims processing
- Payroll processing
- Payment processing

- Cloud ERP service
- Data centre colocation
- IT systems management

SOC2/SOC3 operational controls

- Enterprise cloud e-mail
- Cloud collaboration
- Software-as-a-service-(SaaS)-based HR services
- SaaS enterprise system housing third-party data
- Any service where topics such as security, availability, and privacy are areas of concern

Applicability to different types of outsourced services

Using the table above will help to determine what type of SOC report is most applicable regarding certain controls and services. Starting at the left end of the table, there are services that are clearly financial reporting oriented, and where it is likely SOC1 reports will be requested, and provided. These include financial services as well as processing for healthcare claims, payroll, payment and financial transaction processing.

In addition, there may be some cases where users require more detail on security or availability. In these cases, the service provider might provide a SOC1 report for ICOFR purposes, and a SOC2 or SOC3 report to address security/availability assurance needs if the demand for such reports or the burden of accommodating users' security audits is great enough.

In the middle of the table are services that do not neatly fit into one category or the other. Depending on the specific nature of services provided, and user needs, SOC1, and/or SOC2 may be most applicable. For example:

- A **cloud-based ERP service** historically would have provided a SAS 70 report to their clients because it provided a core financial reporting service to users. It is likely that it would continue to provide a SOC1 report for that same reason. However, it may also have a need to provide a SOC2 or SOC3 security, and availability report to address user assurance needs specific to cloud services.
- Many **data centre colocation** providers have historically completed SAS 70 examinations limited to physical and environmental security controls. However, most data centre providers host much more than just customers' financial systems. As a result, leading providers are moving toward SOC2 security reporting. Some service providers incorporate supporting environmental security controls within their SOC2 security report, whereas others also address the Availability Criteria depending on the nature of their services.
- For **IT systems management**, which can include general IT services provided to a portfolio of users as well as customised services provided to specific users, SOC1 or SOC2 reporting could be applicable, depending on whether users' assurance needs are more focused on ICOFR or security/availability.

At the other end of the spectrum, there are services that are operational, and technology focused with very little, if any, direct connection to users' ICOFR.

For example, these types of outsourced services are unlikely to be included within a public company's financial reporting scope. Users of these services are typically most concerned about the security of their data, and availability of these systems. This would typically be addressed by a SOC2 or SOC3 report covering Security, and Availability. Where applicable, SOC2/SOC3 reports can also cover Confidentiality, Processing Integrity, and/or Privacy as well. SOC2 is also potentially applicable for any organisation that is storing, and processing sensitive third-party data.

Where there is a need to demonstrate to third parties that effective Security, and Confidentiality controls are in place to protect information, SOC2, and SOC3 reports provide a mechanism for providing this assurance. Through the system description in the report, the organisation clearly describes the boundary of the "system", and the examination is then performed based on the defined Trust Services Criteria.

Leading practices for user organisation adoption of SOC2/SOC3

Users should assess the impact to their key outsourced vendors, and whether having SOC2/SOC3 assurance can provide benefits from a vendor risk management, and business perspective. Key activities may include the following:

Key Activities	Description
Inventory vendor relationships	• Inventory existing outsourced vendor relationships to determine where the organisation has obtained, and requires third-party assurance going forward.
Assess vendor risks	• Assess the key risks associated with significant outsourced vendors (e.g., Security, Availability, other risks).
Identify relevant reports	• Assess whether SAS 70 or other reports have been obtained in the past. • Determine whether SOC1 reports should be requested going forward. • Determine whether detailed SOC2 or summary level SOC3 reports are required for key outsourced vendors. Also determine which Principles should be covered within the SOC2/SOC3 reports (e.g., Security, and Availability or other Principles as well).
Contractual provisions	• Assess what, if any, specific audit reports are required by contract, and whether contracts have right to audit clauses. • Determine how any historical SAS 70 references should be updated to new SOC reports. • Determine whether SOC2/SOC3 reports should be required by contract.

Key Activities	Description
Vendor monitoring	• Determine the frequency with which key outsourced vendors' will be assessed. • Build the process of obtaining and reviewing SOC reports and following up on any areas of concern into the vendor monitoring process.
Vendor due diligence	• Consider requesting relevant SOC reports as part of the due diligence process for assessing and onboarding new outsourced service providers.
Communication plan	• Where assurance reports are desirable, key points should be communicated and confirmed with the service providers: – Scope of the system covered – Specific report to be provided (ISAE 3402/SOC1, SOC2, SOC3) – Type of report to be provided and period covered (i.e., Type 2 for a specified period, or in certain cases, Type 1 as of a specified point in time) – Control domains covered (included control objectives for ISAE 3402/SOC1, included Principles for SOC2/SOC3) – Existence of any key supporting subservice providers (e.g., data centre providers, IaaS providers) and whether they are included in scope – Expected report delivery date.

Key considerations when evaluating assurance reports

Users should consider the following factors when evaluating assurance reports obtained from service providers:

Topic	Evaluation Considerations
Type of Report	• Determine whether the report is a ISAE 3402/SOC1, SOC2, SOC3 or other report.
Period of Coverage	• Determine whether the report is a Type 1 or a Type 2, what period of time is covered, and whether the period of coverage meets the user's needs.
Opinion	• Assess whether the service provider received an unqualified (clean) opinion or if qualifications (failed control objectives or criteria) were noted. • Assess the impact of any such qualifications.
Audit Firm	• Assess whether the firm has a good reputation for providing the type of assurance services.
Scope	• Review the system description and opinion to confirm whether the report scope is relevant and corresponds to the services/locations relevant to the user.
Subservice Organisations	• Review the opinion and system description to determine whether subservice organisations are used and whether they are included or excluded from the scope of the report. • Assess whether additional assurance is needed where key subservice organisations are carved out of scope.
Control Criteria/ Objectives	• Assess whether the Control Objectives used for ISAE 3402/SOC1 and the Principles covered for SOC2/SOC3 sufficiently cover the user's assurance needs and requirements.
Complementary User Entity Controls	• Review any identified complementary user entity controls and determine whether the user has procedures in place to address these, to the extent applicable.
Description of Control Activities	• For ISAE 3402/SOC1 and SOC2, review the description of control activities and assess whether they are at the expected level of granularity.
Test Procedures	• For ISAE 3402/SOC1 and SOC2, review the auditor's test procedures and assess whether specific tests were adequate.
Test Results	• For ISAE 3402/SOC1 and SOC2, review any test exceptions noted in the report and management's responses (if provided) and assess whether there is an impact to the user organisation and if any follow up with the service provider is required.
Changes During the Period	• Assess whether any significant changes in systems, subservice providers, or controls are noted and any impact to the user.

Leading practices for service provider adoption of SOC2/SOC3

With the retirement of the SAS 70 report in 2011, increasing market awareness of the new SOC2/SOC3 reporting options and the emergence of more technology focused services such as cloud, users will be revisiting their needs for assurance reports. Based on numerous industry meetings and client discussions, there has been a positive reaction to the new SOC2/SOC3 reports in situations where users are concerned about security, availability and privacy. We recommend that service providers proactively evaluate their need to provide a SOC2/SOC3 report to users and develop their plan to move to the new SOC2/SOC3 standards, where appropriate.

Key elements of a plan to assess and address the impact of the new SOC2/SOC3 standards may include the following:

Topic	Applicability
Inventory current requirements	• Inventory the historical set of parties who have received assurance reports • Inventory contractual commitments to provide assurance reports • Inventory the recent requirements of users and prospects (e.g., as reflected in security questionnaires)
Determine go forward requirements	• Assess the extent to which users and prospects rely upon Service Organisation Control reports for financial reporting purposes versus governance/operational/security purposes • Assess the portfolio of current and planned services and the associated risks to users • Determine which report(s) will best meet the needs of their users and potential users
Address the impact of new standards	• Re assess the existing report scope to consider the requirements of ISAE 3402/SOC1 • For reports that are transitioning to SOC2, determine which principles should be covered • Map identified controls (from past SAS 70 reports or other control documentation) to the SOC2/SOC3 requirements and identify any gaps • Based on the gap analysis, determine the timeline for SOC2/SOC3 completion. For example, in some cases it may make sense to cover Security first but defer inclusion of additional Principles until later reports • Develop a plan to address identified gaps and prepare for the formal SOC2/SOC3 audit
Communication plan	• Define a communication plan for informing key users of the service provider's audit plans for the current year • Develop FAQs/talking points for the broader team (User Service, Sales/ Marketing, IT, etc.) to help them explain the service provider's audit plans and effectively answer any user questions

For service providers that have not previously completed an audit, there is typically a two phase process to prepare for and complete the SOC2/SOC3 examination. The following diagram summarises our phased approach for first time audits. We start with an Audit Preparation phase where we collaborate with the service provider and provide guidance to set the stage for a successful audit. The Audit phase then builds upon the understanding of the service provider's architecture and controls that was established in the Audit Preparation phase.

Audit Preparation

- Define audit scope, and overall project time line
- Identify existing or required controls through discussions with management, and review of available documentation
- Perform readiness review to identify gaps requiring management attention
- Communicate prioritised recommendations to address any identified gaps
- Hold working sessions to discuss alternatives, and remediation plans
- Verify that gaps have been closed before beginning the formal audit phase
- Determine the most effective audit, and reporting approach to address the service provider's external requirements

Audit

- Provide overall project plan
- Complete advance data collection before on-site work to accelerate the audit process
- Conduct on-site meetings, and testing
- Complete off-site analysis of collected information
- Conduct weekly reporting of project status, and any identified issues
- Provide a draft report for management review, and electronic, and hard copies of the final report
- Provide an internal report for management containing any overall observations, and recommendations for consideration

Point of view on the use of SOC reports

Historically, many organisations that use outsourced services have asked for SAS 70 reports. Few organisations understood or acknowledged that the SAS 70 report was designed for a specific purpose – to help users and their auditors to rely upon the controls over a service provider in the context of the users' financial statement and internal control over financial reporting audits. Many of these users were concerned about areas such as security, availability and privacy with little or no regard for financial reporting implications. Despite the existence of other IT/security-focused assurance tools (e.g., ISO 27001, WebTrust, SysTrust, etc.) that were arguably better suited for the purpose, users continued to ask for SAS 70 reports and service providers and their auditors accommodated.

With the replacement of the SAS 70 report by SOC reports, the professional guidance is now clear.

- In the majority of cases, service providers that provide core financial processing services (e.g. payroll, transaction processing, asset management, etc.) moved to the ISAE 3402/SOC1 report in 2011.
- IT service providers that have no impact or an indirect impact on users' financial reporting systems have started to move to the SOC2 report.
- The SOC3 report has been used where there is a need to communicate a level of assurance to a broad base of users without having to disclose detailed controls and test results. Some organisations may complete a combined SOC2/SOC3 engagement with two reports, geared for different constituencies.

Whichever report is relevant to the service organisation, the SOC report set now offers a wide reaching assurance tool that gives both service organisations and user organisations a medium to demonstrate control and offers comfort around the service industry. With the increase focus on transparency and requirements around demonstrable control, this is the most pragmatic and internationally recognised solution and their use will continue to grow.

Contact us

Stephan Claes
Partner, KPMG Advisory
T: +32 2 708 48 50
E: sclaes3@kpmg.com

Dirk Timmerman
Executive Director, KPMG Advisory
T: +32 2 708 43 59
E: dtimmerman@kpmg.com

kpmg.be