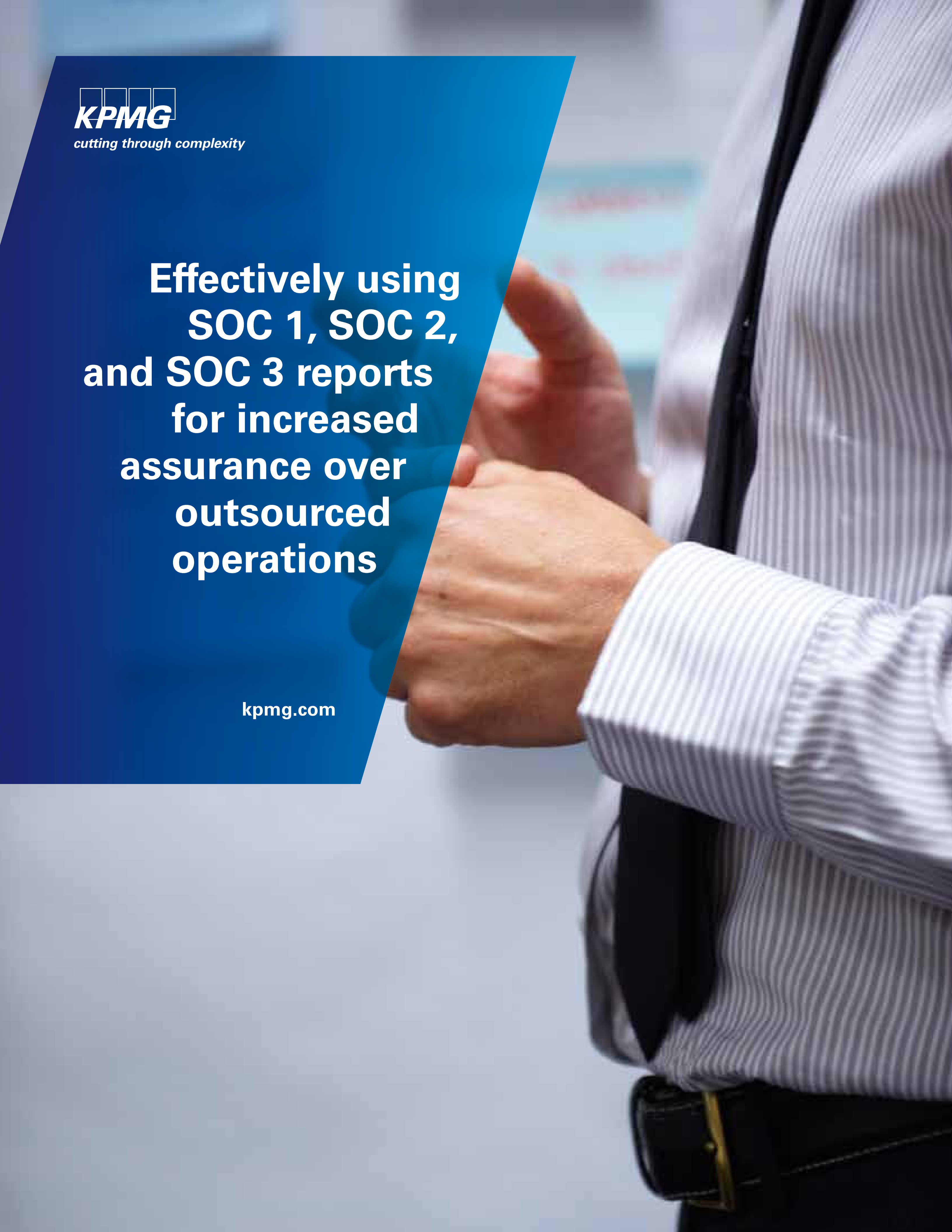
KPMG

cutting through complexity

Effectively using SOC 1, SOC 2, and SOC 3 reports for increased assurance over outsourced operations

kpmg.com



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.

This paper provides user organizations (customers) and service providers an overview of SOC 2/SOC 3, and guidance for the application of SOC 2/SOC 3 reporting, including the following topics:

Overview of SOC 2/SOC 3 reporting

- SOC reporting options
- SOC report types
- Contrasting the scope of SOC 2/SOC 3, and SOC 1 reports
- SOC 2/SOC 3 Principles
- SOC 2/SOC 3 Criteria
- Applicability to different types of outsourced services
- Contrasting the level of detail provided by SOC 2, and SOC 3 reports
- SOC report structure

Application of SOC 2/SOC 3 reporting

- Applicability to different types of outsourced services
- Leading practices for user adoption of SOC 2/SOC 3
- Key considerations when evaluating assurance reports
- Leading practices for service provider adoption of SOC 2/SOC 3
- Point of view on the use of SOC reports

Overview of SOC 2/SOC 3 reporting

SOC reporting options

In the past, the SAS 70 report was intended to assist service organizations' users and their auditors in the context of a financial statement audit. Now, three types of SOC reports (summarized below) have been defined to replace SAS 70 and address a broader set of specific user needs—such as addressing security, privacy, and availability concerns. Additionally, service organizations are looking for better ways to provide assurance over their control environments.

	Internal control over financial reporting (ICOFR)	Operational controls	
	SOC 1*	SOC 2	SOC 3**
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 – Privacy. Applicable to a broad variety of systems	

* *Sometimes also referred to as an SSAE 16, AT 801 or ISAE 3402 report*

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

SOC report types

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 six 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 organization required a period of time report covering Security, and Availability for a particular system, the user organization would request a SOC 2 Type 2 Security, and Availability report from the service provider. If the user organization required a period of time report covering ICOFR controls for a particular system, the user organization would request a SOC 1 Type 2 report of that system from the service provider.

Contrasting the scope of SOC 2/SOC 3 versus SOC 1 reports

The table below compares, and contrasts the required focus, scope, and control domains covered by SOC 2/SOC 3 versus SOC 1 reports.

	SOC 1	SOC 2/SOC 3
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 information technology general controls *Note: In certain cases, a SOC 1 report might cover supporting IT controls only, depending on the nature of services provided.	• Security • Availability • Confidentiality • Processing Integrity • Privacy
Level of standardization	• 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 predefined Criteria are used rather than control objectives.

SOC 2/SOC 3 principles

SOC 2, and SOC 3 reports use the 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 ICOFR. Principles, and Criteria are specifically defined for Security, Availability, Confidentiality, Processing Integrity, and Privacy (see the table on the following page). This has been done in a modular way so that a SOC 2 or SOC 3 report could cover one or more of the Principles depending on the needs of the service provider, and its users.

In contrast, SOC 1 reports require a service organization to describe its system, and define its control objectives and controls that are relevant to users' internal control over financial reporting. A SOC 1 report generally should not cover services or control domains that are not relevant to users from an ICOFR perspective, and it specifically cannot cover topics such as disaster recovery and privacy.

Domain	Trust Services Principle	Applicability
Security	• The system is protected against unauthorized 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, nonfinancial 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 SAS 70 or SOC 1 reports
Confidentiality	• Information designated as confidential is protected as committed or agreed.	• Most applicable where the user requires additional assurance regarding the service provider's practices for protecting sensitive business information
Processing Integrity	• System processing is complete, accurate, timely, and authorized.	• Potentially applicable for a wide variety of non-financial, and financial scenarios wherever assurance is required as to the completeness, accuracy, timeliness, and authorization 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 generally accepted 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

SOC 2/SOC 3 Criteria

For first-time SOC 2 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 organization already has a security program based on a standard such as ISO 27001 or if it 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 on this page summarizes 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 summarized 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 authorization 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 organizations 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 SOC 2 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 SOC 2, and SOC 3 reports

As discussed earlier, SOC 2 and SOC 3 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 SOC 2 reporting or summary level SOC 3 reporting will satisfy the needs of its users. In both cases, a detailed examination is performed based on the specific Criteria; however, the SOC 2 report includes detailed information on the service provider's controls, and the auditors' individual test procedures and results.

	SOC 2	SOC 3
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	• SOC 2 is more flexible than SOC 3 for the service provider in that it permits carve-out of supporting services provided by subservice providers. • SOC 2 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.	• SOC 3 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, it may choose to display the SOC 3 seal on its Web site which links to the SOC 3 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).	• SOC 3 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, SOC 3 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 SOC 3 seal until the issue(s) are corrected, and reaudited.

SOC report structure

The following table compares and contrasts the structure and contents of SAS 70 and SOC reports. Each of these reports can cover 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	SOC 1	SOC 2	SOC 3
Auditor's Opinion	Auditor's Opinion	Auditor's Opinion	Auditor's Opinion
–	Management Assertion	Management Assertion	Management Assertion
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 SOC 1

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
–	• –	–

SOC 2

Security Principle: The system is protected against authorized 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 policies to responsible parties, and authorized users.

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

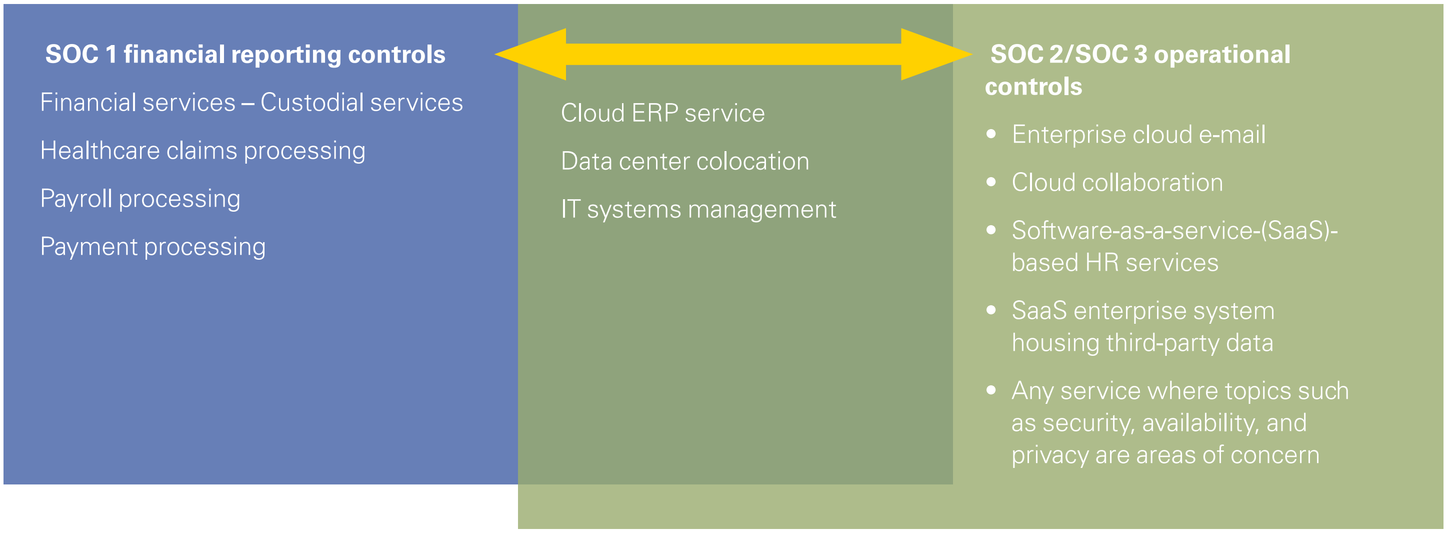
3.0 Procedures: The entity uses procedures to achieve its documented system security objectives in accordance with its defined policies.

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 SOC 2/SOC 3 reporting



SOC 1 financial reporting controls

Financial services – Custodial services

Healthcare claims processing

Payroll processing

Payment processing

Cloud ERP service

Data center colocation

IT systems management

SOC 2/SOC 3 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

The following content refers to the table above, which has been developed to help determine what type of SOC report is most applicable regarding certain controls and services. Starting at the left end of the spectrum, there are services that are clearly financial reporting oriented, and where it is likely SOC 1 reports will be requested, and provided. These include financial services as well as processing for healthcare claims, payroll, and payment.

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 SOC 1 report for ICOFR purposes, and a SOC 2 or SOC 3 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 don't neatly fit into one category or the other. Depending on the specific nature of services provided, and user needs, SOC 1, and/or SOC 2 may be most applicable. For example:

- A cloud-based ERP service historically would have provided a SAS 70 report because it provided a core financial reporting service to users. It is likely that it would continue to provide a SOC 1 report for that same reason. However, it may also have a need to provide a SOC 2 or SOC 3 security, and availability report to address user assurance needs specific to cloud services.
- Many data center colocation providers have historically completed SAS 70 examinations limited to physical and environmental security controls. However, most data center providers host much more than just customers' financial systems. As a result, leading providers are moving toward SOC 2 security reporting. Some service providers incorporate supporting environmental security controls within their SOC 2 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 customized services provided to specific users, SOC 1 or SOC 2 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 Sarbanes-Oxley (SOX) 404 scope. Users of these services are typically most concerned about security of their data, and availability of these systems, which can be addressed by a SOC 2 or SOC 3 report covering Security, and Availability. Where applicable, SOC 2/SOC 3 reports can cover Confidentiality, Processing Integrity, and/or Privacy as well. SOC 2 is also potentially applicable for any organization 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 that information, SOC 2, and SOC 3 provide a mechanism for providing assurance. Through the system description in the report, the organization clearly describes the boundary of the "system", and the examination is then performed based on the defined Trust Services Criteria.

Leading practices for user organization adoption of SOC 2/SOC 3

Users should assess the impact to their key outsourced vendors, and whether having SOC 2/SOC 3 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 organization 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 SOC 1 reports should be requested going forward. • Determine whether detailed SOC 2 or summary level SOC 3 reports are required for key outsourced vendors. Also determine which Principles should be covered within the SOC 2/SOC 3 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 SOC 2/SOC 3 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 (SOC 1, SOC 2, SOC 3) – 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 SOC 1, included Principles for SOC 2/SOC 3) – Existence of any key supporting subservice providers (e.g., data center providers, IaaS providers), and whether they are included in scope – Expected report delivery date.

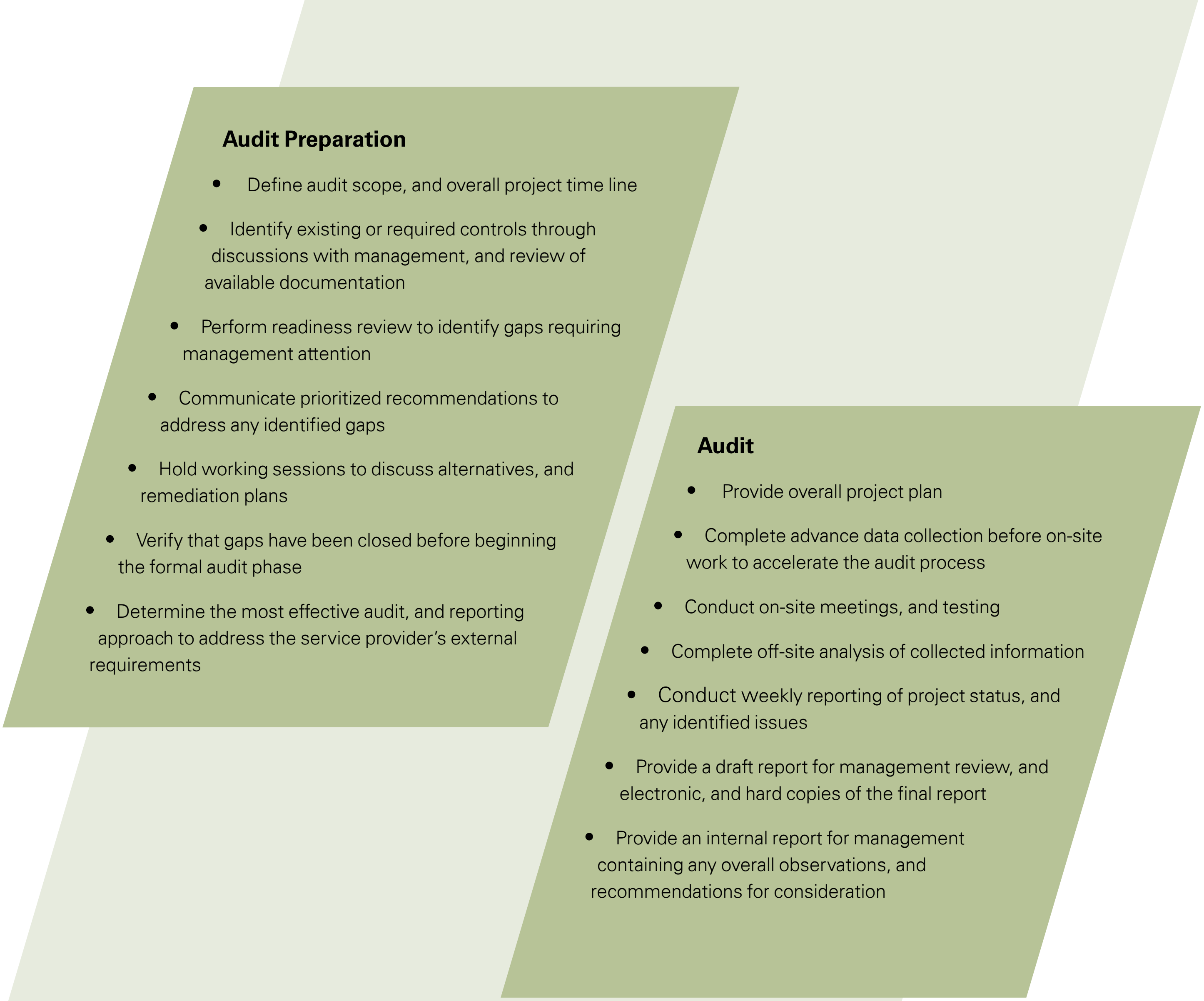
Leading practices for service provider adoption of SOC 2/SOC 3

With the retirement of the SAS 70 report in 2011, and increasing market awareness of the new SOC 2/SOC 3 reporting options, users will be revisiting their needs for assurance reports, and communicating those requirements at contract renewal time, as they negotiate changes to contracts, and as they complete their vendor risk management activities. Based on numerous industry meetings, and client discussions, there has been a positive reaction to the new SOC 2/SOC 3 reports in situations where users are concerned about security, availability, and privacy. We recommend that service providers proactively evaluate their need to provide a SOC 2/SOC 3 report to users, and develop their plan to move to the new SOC 2/SOC 3 standards, where appropriate.

Key elements of a plan to assess, and address the impact of the new SOC 2/SOC 3 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 SOC 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	• Reassess the existing report scope to consider the requirements of SOC 1 • For reports that are transitioning to SOC 2, determine which Principles should be covered. • Map identified controls (from past SAS 70 reports or other control documentation) to the SOC 2/SOC 3 requirements, and identify any gaps. • Based on the gap analysis, determine the time line for SOC 2/SOC 3 completion. For example, in some cases it may make sense to cover Security in 2011 but defer inclusion of additional Principles until 2012. • Develop a plan to address identified gaps, and prepare for the formal SOC 2/ SOC 3 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 SOC 2/SOC 3 examination. The following diagram summarizes 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 prioritized 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 organizations that use outsourced services have asked for SAS 70 reports. Few organizations 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 ICOFR 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., WebTrust, SysTrust, ISO 27001, 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 with SOC reports, the professional guidance is now clear. The AICPA has also provided messaging to clearly explain the different types of SOC reports, and where they are applicable.

In the majority of cases, service providers that provide core financial processing services (e.g., payroll, transaction processing, asset management, etc.) moved to the SOC 1 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 SOC 2 report. The SOC 3 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 organizations may complete a combined SOC 2/SOC 3 examination with two reports, geared for different constituencies.

Contact us

Sandy Torchia
Partner, Risk Consulting
Americas SOC Reporting Leader
T: 267-256-2720
E: storchia@kpmg.com

Mark Lundin
Partner, Risk Consulting
U.S. SOC 2/SOC 3 Reporting Leader
T: 415-963-5493
E: mlundin@kpmg.com

kpmg.com

The information contained herein is of a general nature, and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate, and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.