KPMG

cutting through complexity

Overview of Service Organization Control (SOC) Reports

Sacramento Chapter Presentation

February 21, 2013

Agenda

- Introduction
- Overview of SOC reporting options
  - Intended subject matter and scope
  - SOC report structure
  - Target audience
- Application to various outsourced services
- Considerations for service providers
  - Which report(s) to provide
  - Scoping reports
  - Audit and reporting process
- Considerations for user organizations
  - Which report(s) to request
  - Subject matter and scoping
  - How to review and use SOC reports

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.
- Many organizations have historically relied upon Statement on Auditing Standards (SAS) 70 reports to gain broad comfort over outsourced activities. 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.
- The professional guidance is now clear—with the retirement of the SAS 70 report in 2011, a suite of Service Organization Control (SOC) reports have been defined by the AICPA to replace SAS 70 reports, and more clearly address the assurance needs of the users of outsourced services.
- Three types of SOC reports – SOC 1, SOC 2, and SOC 3 – have been defined to address a broader set of specific user needs.

Overview of SOC reports

	SOC 1 *	SOC 2 / SOC 3 **
Summary	▪ 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 operational risks and controls related to security, availability, confidentiality, processing integrity, and privacy. ▪ Applicable to a broad variety of systems/services.
Required focus	▪ Internal control over financial reporting (ICOFR)	▪ 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	The five key components of a system ▪ Infrastructure - The physical and hardware components of a system (facilities, equipment, and networks) ▪ Software - The programs and operating software of a system (systems, applications, and utilities) ▪ Procedures - The automated and manual procedures involved in the operation of a system ▪ People - The personnel involved in the operation and use of a system (developers, operators, users, and managers) ▪ Data - The information used and supported by a system (transaction streams, files, databases, and tables)

**** 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***

Overview of SOC reports, cont.

	SOC 1	SOC 2 / SOC 3
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.	The Trust Services Principles. ▪ Security ▪ Availability ▪ Confidentiality ▪ Processing Integrity ▪ Privacy
Treatment of subservice organizations	▪ Carve-out or Inclusive method allowed	▪ SOC 2 – carve-out or inclusive method ▪ SOC 3 – only inclusive method allowed
Level of Standardiz-ation	▪ 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.

Trust Services Principles used in SOC 2 / SOC 3

	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 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

Trust Services Principles used in SOC 2 / SOC 3, cont.

	Trust Services Principle	Applicability
Processing Integrity	▪ System processing is complete, accurate, timely, and authorized.	▪ Potentially applicable for a wide variety of nonfinancial, 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

Criteria areas for Trust Services Principles

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

Availability

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

Processing Integrity

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

Confidentiality

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

Privacy

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

SOC Reporting

- Reports most commonly cover the design and effectiveness of controls (a Type 2 report) for a 12-month period of activity, with continuous coverage from year to year.
- Reports 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.
- Reports may also cover only the design of controls at a specified point in time (a Type 1 report); this often used for a new system/service or for the initial examination (audit) of a system/service.
- 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 a user organization required a period of time report covering ICOFR for a particular system, the user organization would request a SOC 1 Type 2 report for that system from the service provider.

SOC report structure

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
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*

SOC report structure, cont.

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
–	–	• –	–

Intended SOC Report users and distribution

	SOC 1	SOC 2	SOC 3
Intended Users	▪ Auditor to Auditor communication on internal controls relevant to financial reporting ▪ Detailed report for existing customers and their financial statement auditors	▪ Detailed report for customers and specified parties	▪ Short report that can be widely distributed ▪ Option to display a web site seal (if unqualified opinion) 
Distribution	▪ “Restricted use” report ▪ Limited distribution	▪ Likely a restricted use report ▪ Distribution limited to those with adequate understanding of the criteria	▪ General use report ▪ Able to be widely distributed

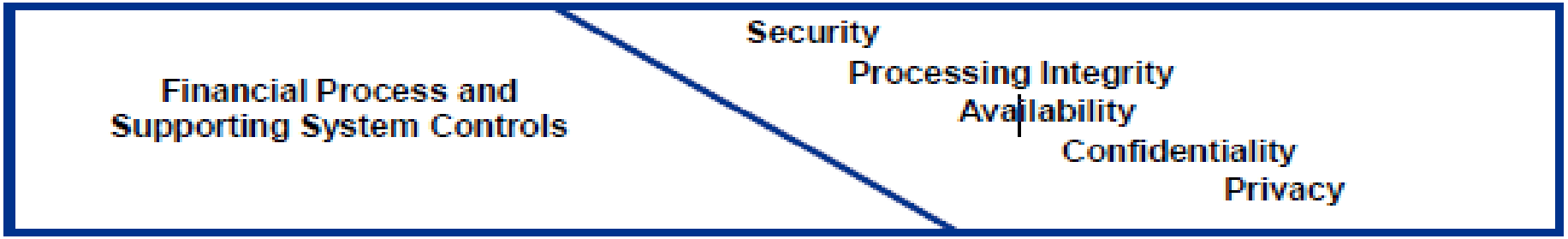
SOC Reports for commonly outsources services

SOC1 Financial Reporting Controls ⟷ **SOC2/SOC3 Operational Controls**

- **Financial services**
- **Asset management and custodial services**
- **Healthcare claims processing**
- **Payroll processing**
- **Payment processing**

- **Cloud ERP service**
- **Data center co-location**
- **IT systems management**

- **Cloud-based services (SaaS, PaaS, IaaS)**
- **HR services**
- **Security services**
- **Email, collaboration and communications services**
- **Any service where customers' primary concern is security, availability or privacy**



Example: Financial Services – Common Concerns

- Regulatory pressures to demonstrate sound vendor risk management (e.g., OCC, Fed, Consumer Financial Protection Bureau)
- Regulatory and industry requirements (FFIEC, Gramm-Leach-Bliley, PCI standards)
- Protection of sensitive transaction and customer data
- Availability of critical outsourced systems
- Limited resources to analyze responses to detailed questionnaires or perform vendor audits

Example: Financial Services – Scenario & Use of SOC 2

- Online transaction processor with financial institution and business partner security requirements based on ISO 27001 and PCI.
- As shown below, the Financial Services Provider can include additional information in the Other Information section of the SOC2 report to demonstrate alignment of controls with the requirements of a specific standard (e.g., ISO 27001/27002, FFIEC standards, PCI) or common vendor security questionnaire topics.

SAMPLE – Relation of Service Provider's Controls to ISO 27001/27002 Control Objectives

Service Provider has developed its controls to align with the ISO 27001/27002 control objectives. Included below is a mapping of the ISO 27001/27002 topics to related Service Provider controls covered in this report.

ISO 27001/27002 Control Objective Topics	SOC2 Criteria	Related Service Provider Controls
A.5.1 Information security policy	1.01, 1.02	ABC has information security policies which have been approved by management, published and communicated to employees, and address each of the criterion 1.02 topics. Changes to policies require approval from management.
A.6.1 Internal organization	1.03	ABC's information security group is responsible for setting security policy, assessing security and availability risks, performing IT security and control assessments, and facilitating security initiatives.
A.6.2 External parties	1.02	Control description included.
…		…

Example: Healthcare Services – Common Concerns

- Protection of protected health information (PHI), personally identifiable information (PII), and other sensitive information.
- Compliance with regulatory requirements and data security and privacy standards (HITECH, HIPAA)
- Vendor controls/business associate agreements (BAA)
- Availability of critical outsourced systems

Example: Healthcare Services – Scenario & Use of SOC 2

- Healthcare claims processor and a business partner requirement based on HIPAA.
- As shown below, the Healthcare Services Provider can include additional information in the Other Information section of the SOC 2 Report to illustrate how their controls align with relevant industry standards (HIPAA in this case).

SAMPLE – Relation of Service Provider's Controls to HIPAA Security Standards

Service Provider has developed its controls to align with the HIPAA security standards. Included below is a mapping of the HIPAA security topics to related Service Provider controls covered in this report.

HIPAA Security Topics	SOC2 Criteria	Related Service Provider Controls
Administrative safeguards		
Security Management Process	3.01, 3.02 4.01, 4.02, 4.03	A formal risk assessment process is in place for the ABC service. The Security team performs risk assessments on an annual basis or whenever there is a major change to the ABC service. Risk assessment results are shared with senior management and remediation actions are identified and applied to address noted risks in a timely manner. ABC utilizes an Intrusion Detection System (IDS) for intrusion detection and a central log server is used to capture IDS events. Security team members continuously monitor these consoles and act on alerts. …
Assigned Security Responsibility	1.03	ABC's information security group is responsible for setting security policy, assessing security and availability risks, performing IT security and control assessments, and facilitating security initiatives.
…	…	…
Physical safeguards	#.##, #.##	Control descriptions included.
Technical safeguards	#.##, #.##	Control descriptions included.

Example: Cloud Service Provider (CSP) – Common Concerns

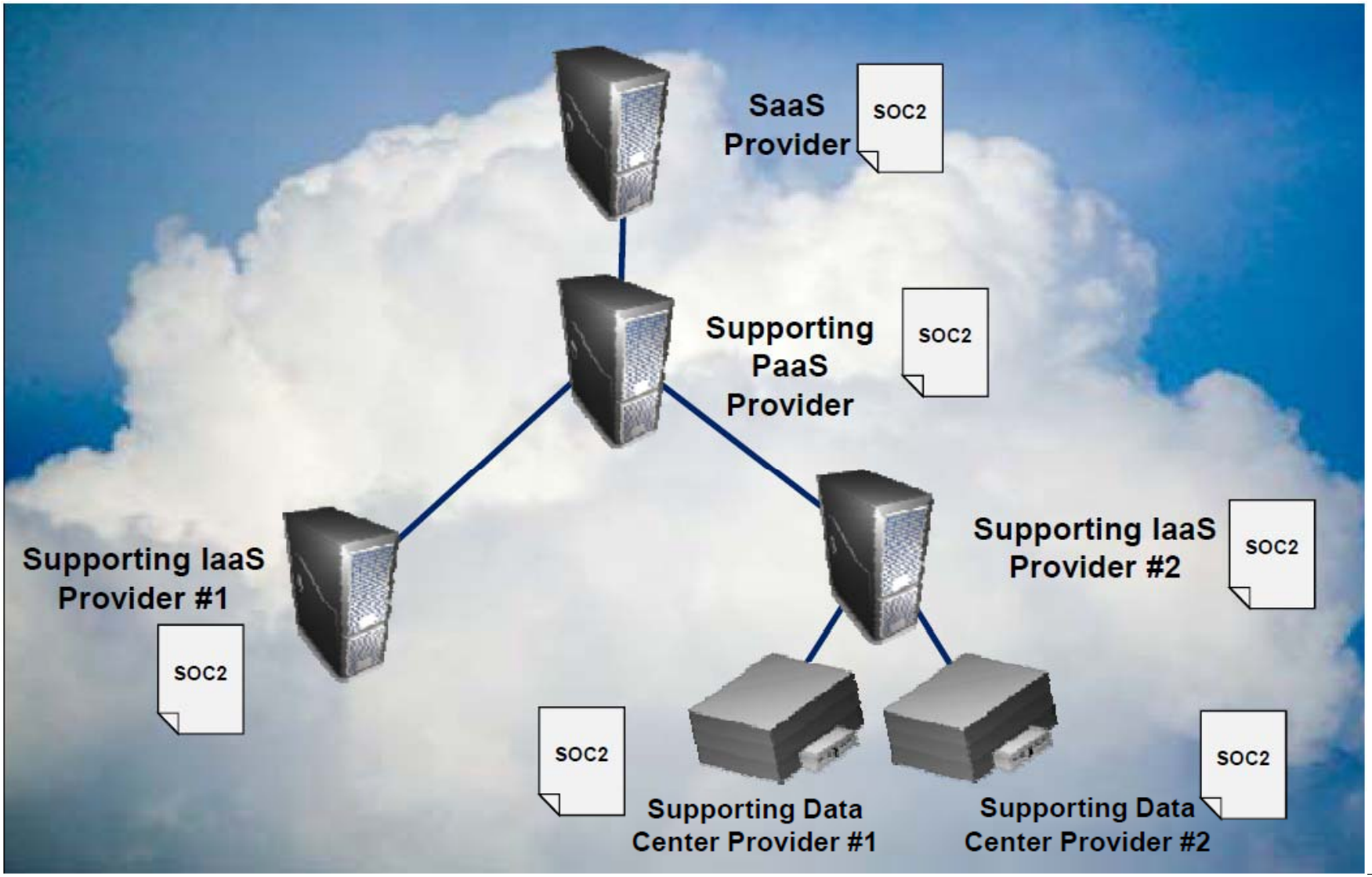
Information Security Management System

- Security policy
- Organization of Information Security
- Asset Management
- Human Resources Management
- Physical & Environmental Security
- Communications & Operations Management
- Access Control
- Information Systems Acquisition, Development, and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

Areas of Added Focus

- Data Protection / Segregation / Confidentiality (B2B)
- Encryption Standards
- Configuration Management
- Authentication to Cloud
- Logging and Real-Time monitoring
- Vendor Integration (SaaS/ PaaS/ IaaS layers)
- Privacy (B2C)

Example: CSP – Common Concerns, Multi-vendors



Example: CSP – Scenario & Use of SOC 2

- Online application used in a non-financial business process
- Could have business partner requirements based on ISO 27001, CSA Cloud Controls Matrix (CCM), FISMA/FedRAMP, or other
- The CSP can include additional information in the Other Information section of the SOC2 report to demonstrate alignment of their controls with the requirements of the specific standard(s) or common vendor questionnaire topics.

Leading practices for *service provider* adoption of SOC reporting

Key Activities	Description
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.

Leading practices for *service provider* adoption of SOC reporting, cont.

Key Activities	Description
Address the impact of new standards	▪ Reassess the existing report scope to consider the requirements of SOC1 ▪ For reports that are transitioning to SOC 2, determine which Principles should be covered. ▪ Map identified controls (from past SAS 70 / SOC 1 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 year 1 and defer inclusion of additional Principles into future. ▪ 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.

A two-phased approach to auditing and reporting *

- For service providers that have not previously completed an examination (aka audit), there is typically a two-phase process to prepare for and complete it.
  - ***Audit Preparation***: We collaborate with the service provider, and provide guidance to set the stage for a successful.
  - ***Audit*** *:* Builds upon the understanding of the service provider's architecture and controls that was established in the Audit Preparation phase.

Phase 1: 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

Phase 2: 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 regular 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

** Service auditors' processes vary and your experience my differ.*

Leading practices for *user organization* adoption of SOC reporting

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).

Leading practices for *user organization* adoption of SOC reporting, cont.

Key Activities	Description
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.
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 on-boarding new outsourced service providers.

Leading practices for *user organization* adoption of SOC reporting, cont.

Key Activities	Description
Communication plan	▪ Where assurance reports are desirable, key points should be communicated, and confirmed with the service providers: – Scope of the system covered (Clear definition of the system that should be included within scope) – Specific report to be provided (SOC 1, SOC 2, SOC 3) - For SOC1, convey the general scope of control objectives that should be covered - For SOC2/SOC3, convey which Principles should be covered – Type (1 or 2) 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) – Existence of any key supporting subservice providers (e.g., data center providers, IaaS providers), and whether they are included in scope - Determine if additional reports are required (e.g., a SOC2 report from the supporting IaaS provider if the service provider's SaaS solution runs on that infrastructure). – Expected report delivery date.

Leading practices for *user organization* evaluation of SOC reports

Topic	Evaluation Consideration
Scope	▪ Is the scope of services and locations included in the report relevant based on the services YOU receive from the service provider?
Type of Report	▪ Is the report a SOC 1, SOC 2, SOC 3 or other type of report? ▪ Is the report a point in time (Type 1) or a period of time (Type 2) report?
Period of Coverage & Report Timing	▪ How well do the period of coverage and report timing meet your needs?
Opinion	▪ Is the opinion unqualified (clean) or was it qualified? ▪ If qualified, what control objectives/criteria were not achieved and is that relevant to the Services YOU receive?
Audit Firm	▪ Does the audit firm issuing the opinion have a good reputation for providing this type of assurance services?
Subservice Organizations	▪ If subservice organizations are used, are controls over these operations included (inclusive method) or excluded (carve-out method) from the scope of the report? ▪ If excluded, is additional assurance needed from the sub-service organization (e.g. through a separate SOC report from them)?

Leading practices for *user organization* evaluation of SOC reports, cont.

Topic	Evaluation Consideration
Objectives / Principles	▪ Do the selected control objectives or Trust Services Principles sufficiently cover YOUR assurance needs/requirements?
Description of Control Activities	▪ Does the SOC1/SOC2 report provide sufficient detail regarding control activities to meet YOUR needs?
Test Procedures & Results	▪ Are the service auditor's SOC1/SOC2 test procedures sufficient to meet YOUR needs? ▪ If any testing exceptions and management responses are included in the report, is there an impact to the services YOUR organization received and is follow up warranted?
Complementary User Entity Controls	▪ If complementary user entity controls are identified, does YOUR organization have those/similar controls in place?
Changes During the Period	▪ Were there any significant changes in the systems, subservice providers, or controls noted and is there any impact on YOUR organization?
Other Information	▪ Does the report include other helpful information (e.g. how the service provider's controls relate to other industry standards or frameworks such as ISO 27001, CSA's CCM, FISMA, HIPAA, etc)?

Key takeaways

- Three types of SOC reports have been defined to address distinct user requirements:
  - SOC1 focuses on matters relevant to user entities' internal control over financial reporting.
  - SOC 2 / SOC 3 reports apply more broadly to operational controls covering security, availability, confidentiality, processing integrity, and/or privacy across a variety of systems.
  - SOC 2 / 3 can supplement a SOC 1 report by taking a "deeper dive" into key areas.
- Service providers can improve the efficiency and effectiveness of their efforts to meet customer and other compliance requirements and increase the level of assurance provided over the outsourced functions they perform through well thought out SOC reporting.
- Users organizations can improve the efficiency and effectiveness of their vendor risk management programs and increase the level of assurance obtained over the functions they outsource through well thought out SOC reporting.
- SOC2/SOC3 adoption is growing significantly where vendor risk management concerns are more focused on security/confidentiality/availability than financial reporting risks.
- ★ Customers should **not** just "check the box" when requesting SOC reports but rather consider the points previously discussed when evaluating reports

KPMG

cutting through complexity

Thank You

Brian J. Cathcart
Manager, *KPMG* LLP

500 Capitol Mall, Suite 2100
Sacramento, CA 95814
Phone: 916.551.3143
Fax: 916.720.0524
Email: BCathcart@KPMG.com