

Service Organization Control Reports

Allison Morgan
Bureau of Audits
Office of Comptroller Operations

Agenda

- Understanding services provided to your agency by third-parties
 - Service organizations
 - Need for assurance
- Overview of Service Organization Control Reports
 - SOC 1/2/3 Reports
 - Type 1 and Type 2 Reports
 - Examples
- Reviewing Independent Reports
 - Received timely and in accordance with contract
 - Evaluate results and review complementary user entity controls (CUECs)
 - Evaluate deficiencies and ensure corrective action

Service Organizations

- Service organizations provide significant IT support to the Commonwealth
 - When users of a service organization's services (user entities; i.e. agencies) outsource tasks and functions, many of the risks of the service organization (i.e. vendor) become risks of the user entities.
 - SOC reports are issued by service organizations to provide evidence that their control environment is effective.
 - Commonwealth auditors review the SOC reports to obtain an understanding of the effectiveness of agencies' service organizations' control environments.

Service Organizations (Continued)

- Maintain listing of all third-party service organizations
- Monitor contract compliance, including receipt of required SOC reports, audits, SLAs
- Be prepared to respond to external auditor inquiries related to your service organization's controls

Need for Assurance

- Requiring service organizations to provide SOC reports as a means for your agency to gain assurance that controls are in place over your outsourced services
 - Way for the agency to manage their vendor and ensure your data is being captured, processed and maintained effectively and securely, in accordance with related standards
 - Also, way for Commonwealth auditors to obtain an understanding of the effectiveness of agencies' service organizations' control environments
 - If controls in place are effective, the agency and auditors can rely on the outputs from the related system/service providers
 - Effective agency risk management
 - Reduced audit sampling = reduced audit costs

Overview of SOC Reports

Type	Related Standard	Purpose	Examples/notes of when to use
SOC 1 Report	Statement on Standards for Attestation Engagements (SSAE) 16, Reporting on Controls at a Service Organization; AT 801	Detailed description of the system including control objectives and related controls; Reports on controls for financial statement audits	Service provider performs financial transaction processing or supports transaction processing systems; Financial services, asset management, claims processing, payroll processing, payment processing. Most widely used and recognized reporting standard.
SOC 2 Report	AT Section 101; Trust Services Principles and Criteria	Reports on controls related to compliance or operations; Can have self defined objectives, but MUST include at least one (or more) of the five Trust Services Principles	No clear relevant impact to financial reporting controls or transactions can be identified (i.e. – cloud providers, IT hosting reports, HR services, security services, e-mail services, collaboration services, communication services etc.)
SOC 3 Report	AT Section 101; Trust Services Principles and Criteria	Reports on controls related to compliance or operations; Can have self defined objectives, but MUST include at least one (or more) of the five Trust Services Principles	Used to provide public/customers evidence that their data is secure (publicly displayed seal on internet retailer site)

Overview of SOC Reports

Type	Focus	
1	Point in time design-focused	Report on the fairness of the presentation of management’s description of the service organization’s system and the suitability <i>of the design of the controls</i> to achieve the related control objectives included in the description <i>as of a specified date</i>
2	Period of time effectiveness-focused	Report on the fairness of the presentation of management’s description of the service organization’s system and the suitability <i>of the design and operating effectiveness of the controls</i> to achieve the related control objectives included in the description <i>throughout a specified period</i>

Which Report to Use?

- Understand the needs of your user entities, including management and external auditors
 - Are user entities focused on internal control over financial reporting? If so, then a SOC 1 report is most appropriate.
 - Are key compliance and operational controls (such as those related to security, availability, processing integrity, confidentiality, or privacy) of primary interest? If so, then a SOC 2 report may be most appropriate.

Type	Description	Examples/notes of when to use
SOC 1 Report	Detailed description of the system including control objectives and related controls; Internal Control over Financial Reporting	Service provider performs financial transaction processing or supports transaction processing systems; Financial services, asset management, claims processing, payroll processing, payment processing. Most widely used and recognized reporting standard.
SOC 2 Report	Can have self defined objectives, but MUST include at least one (or more) of the five Trust Service Principles	No clear relevant impact to financial reporting controls or transactions can be identified (i.e. – cloud providers, IT hosting reports, HR services, security services, e-mail services, collaboration services, communication services etc.)
Compliance Attestation	Provides opinion on compliance with a set of requirements (requirements can be contractual, statutory/legal, or regulatory). Report can be based on an assessment of internal controls that exist within the entity over the monitoring and compliance of contractual requirements or regulatory requirements.	The practitioner may be engaged to perform agreed-upon procedures to assist users in evaluating the following subject matter (or assertions related thereto)— a. The entity's compliance with specified requirements b. The effectiveness of the entity's internal control over compliance c. Both the entity's compliance with specified requirements and the effectiveness of the entity's internal control over compliance. DPW report on Medicaid is an example.
Performance Audit	Performance Audits are performed against an established set of objectives or standards. Reports provide information and an opinion on the achievement and conclusions relating to the achievement or benchmarking against the established criteria.	Cases where contract includes established criteria/standards/benchmarks.
Agreed-upon Procedure (AUP) Attestation	Engagement performed by an independent auditor in which the auditor conducts an assessment on a set of agreed criteria and procedures. Agreed to by all parties.	Procedures/criteria can be very specific which would limit the cost. Effective for monitoring of activities, and provides an independent assessment and testing.

Type	Description	Examples/notes of when to use
Contract Considerations	Requirements noted within the service providers contract to assist management in gaining assurance over provider's internal control and performance.	
	Are regulatory impacts relevant? If so, are these requirements and liabilities listed in the vendor agreement?	HIPAA, PCI (credit card data)
	Require independent audits to be performed over the services being provided by the service provider (at the cost of the vendor); could add clauses regarding frequency of audits (covered period to coincide with Commonwealth's fiscal year), scope of audits, approvals required by agency, etc. Note that these audits could include any of the above "Independent Audits."	SOC 1 report requirement, SOC 2, Compliance attestation, AUP, Performance audit, Single audit (if federal funding), financial statement audit, or simply the right to audit
Performance Standards	Require service provider to be PCI compliant	credit card vendor
	Defined Key Performance Indicators	Services provided are performance based (set goals for completion of processing tasks)
	Defined Key Performance Indicators; defined performance and operational standards. Must define the related Metrics to be tested against as well as reporting requirements that will evidence meeting of these metrics. Agency must review the reports and determine if met then apply credits/resolve disputes.	Formats are client and project specific. Can include any area of performance on contract responsibilities. Common items for IT hosting/services include: Uptime (availability), Transaction times, Processing volumes, System capacity – Application Access; E-ZPass examples (toll calculation, processing accuracy), Support levels

Reviewing Independent Reports

- Outline requirements in contract
- Ensure required reports are provided to your agency (and timely)
- Evaluate exceptions/deficiencies identified in reports
- Ensure proper remediation of any exceptions/deficiencies

Reviewing Independent Reports (Continued)

- Considerations for evaluating SOC reports
 - Scope – Are your data/services covered?
 - Type – What type of report is it?
 - Period – Does period covered meet your needs?
 - Opinion – Is the opinion unqualified (clean)?
 - Subservice Organizations – If used, are controls over these included in scope or is additional assurance needed from the subservice org?

Reviewing Independent Reports (Continued)

- Considerations for evaluating SOC reports
(continued)
 - Complementary User Entity Controls (CUECs)
 - Evaluate SOC report to determine whether user control considerations are outlined
 - Not all CUECs apply to all user organizations
 - Most CUECs overlap with controls that are already tested
 - Have you implemented them?
 - Have you evaluated their operation and documented them for your external auditors?

Contact Information

Bureau of Audits:

- Allison Morgan allmorgan@pa.gov
- Jennifer Parker jparker@pa.gov
- Julia Thompson julthompson@pa.gov

Links (to open, right click on link and select open hyperlink):

- *Standards for Internal Control in the Federal Government* (Green Book)
<http://www.gao.gov/greenbook/overview>
- [*Management Directive 325.12, Standards for Internal Controls in Commonwealth Agencies,*](#)
- <http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/SORHome.aspx>
- <http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx>