State of Rhode Island - CFO Training
Service Organization Control Reports

June 27, 2019

Office of the Auditor General

Department of Administration – Office of Accounts and Control

State of Rhode Island

Training Objective: To provide State of Rhode Island CFO's with a basic understanding of SOC reports and why they are important, relevant, and useful tools that should be utilized by State financial leaders in evaluating key controls over critical functionalities and monitoring contract compliance by contractors/vendors/fiscal agents.

Agenda

1. What is a Service Organization Control (SOC) Report?
    - Types of reports
    - How to know if a SOC report is available or should be available.
2. How do SOC reports fit into management's overall responsibility for the design, operation and monitoring of controls?
3. Why is it important that I receive, read, and react to information included in SOC reports?
4. Does every contractor/vendor provide a SOC report?

Agenda continued

5. What are the most important areas to focus on when reviewing a SOC report?

   - *Auditor's report/opinion on controls*
   - *Scope of audit including included and excluded functionalities*
   - *Time period covered by audit*
   - *User entity controls*
   - *Sub-service organizations*
   - *Noted exceptions*
   - *Entity management's response and corrective action to noted exceptions*

6. What if I'm having difficulty evaluating whether my activity is included within the scope of the SOC report or if a noted exception impacts my activity?

7. What tools and resources are available to help with the review and consideration of SOC reports?

8. What are the new centralized procedures developed by the Office of Accounts and Control that departments and agencies are required to follow?

Management's responsibility for internal control

Management has responsibility for ensuring:

(1) the adequacy of the design of internal controls, and

(2) controls are in place and operating effectively.

This includes ensuring controls are in place and operating effectively for functions performed by vendors/contractors/fiscal agents.

- This focus on SOC reports and how they should be used in that overall monitoring process is part of an ongoing multi-year objective of having management document and monitor its control structure.

- GAO's "Green Book", *Standards for Internal Control in the Federal Government* tailors the COSO internal control framework to the public environment. The "Green Book" is required for federal agencies and can be useful to other governments when applying COSO principles.

- An internal control framework, such as COSO and/or the Green Book, provides an overall structure for management to design, document, and monitor its internal control policies and procedures.

- The absence of risk assessment and monitoring procedures could lead to significant control deficiencies not being detected and corrected on a timely basis.

OAG audit findings related to SOC reports

Finding – 2018-004 *– Comprehensive Documentation of the State's Internal Control Structure Consistent with the Revised Internal Control Framework*

- Finding includes discussion of making better use of SOC reports within the need for comprehensive documentation of the State's internal controls.

Finding – 2018-017 *– Information Technology – Comprehensive Information Systems Security Policies and Procedures and Periodic Risk Assessments*

- Finding similarly discusses making use of SOC reports within IT monitoring and risk assessment.

What is a Service Organization Control (SOC) Report ?

- SOC reports are prepared by service organization's auditors to perform an examination of controls at the service provider.
- The report includes opinions as to whether the description of the service provider's systems are represented fairly and whether the controls at the service providers are adequate and suitably designed.
- In this case a "system" includes policies, procedures provided to a service user entity.
- Provides for good vendor management
- Provides support for User Entity Controls

SOC Reports

- **SOC 1** - Reports on controls that are relevant to user entities control over financial reporting.
- **SOC 2** - Provides a report about controls at a service organization relevant to the security, availability, or process integrity of the service organization's system, or the confidentiality and privacy of the data processed by the service organization. The report is meant for the user entity, regulators, etc.
- **SOC 3** - Similar to SOC 2, provides less detail of controls related to compliance and operations. They also do not include detailed testing procedures, results or an opinion on the system description. The report is publicly available.

Types of SOC Reports

- Type 1 Report - Is a report on management's description of a service organization's system of processes and related controls and **suitability of the design of those controls - as of a specific date**.

- Type 2 Report -Is a report on management's description of a service organization's system of processes and related controls and the **suitability of the design and operating effectiveness of these controls - throughout the specified period**.

How would I know a SOC Report is Available?

- Contractual requirement?
- Vendor/contractor provides similar service to multiple customers/clients?
- Cloud-based, software-as-a-service or shared data center situation?
- Vendor website details information available to customers/clients?
- Contact client/customer relationship manager and inquire if a SOC report is available to customers?

How do SOC reports fit into management's responsibilities?

- As management, it is your duty to ensure the sufficiency of your internal controls and ensure the adequate data security measures are in place throughout the process (it does not stop at your door).
- The SOC is a tool you can use to ensure the controls at the service organizations that you use are in place are effective-entity level controls
- The report will provide the tools for effective vendor management.

Why is it important I receive, read, and review the information?

- You, as the manager, are held accountable for the service organizations actions.
- You will be expected by the vendor to have certain controls in place-without those controls, your data may fail. The report will help you assess and address the risks associated with the outsources service.
- Look for any exceptions, these could affect the performance of your entity.
- You need to integrate the reviews into an overall vendor management program. You will need to assess your relationship with the vendor if there are deficiencies that they are unwilling or unable to correct.

A report from every vendor?

- This is a judgement call. The answer depends on the nature of the work performed and access to client information.
- If you've outsourced payroll or any other confidential information, yes, you need to ensure we are being protected by proper controls.
- If you have outsourced inmate account control, yes, the vendor is privy to confidential information. You need to be protected.
- If you have outsourced snow plowing, probably not.

Complementary User Entity Controls

- The processes of the Company were designed with the assumption that certain controls would be implemented by user entities. In certain situations, the application of specific controls at user entities is necessary to achieve the overall control objectives included in this report.

- This section highlights the internal control responsibilities that the Company believes should be present for each user entity and has considered in developing its control policies and procedures described in this report. In order for users to rely on the system of controls reported on herein, each user must evaluate its own internal control structure to determine if the following procedures are in place.

- The suggested control activities is intended to address policies and procedures surrounding the interface and communication between the Company and each user entity. **In essence, it clarifies the responsibility for specific controls and control activities between the user-entity and the service provider.**

Examples of SOC reports in State of RI operations

Medicaid – DXC – MMIS claims processing system and related data center

EBT Benefit processing – SNAP, TANF, Unemployment Insurance, TDI benefits

ERSRI:

BNY – Investment custodian and recordkeeper
Morneau Shepell – cloud-based membership/benefit administration system
Ciridian – payroll processor for pension benefits

Trustee services – debt proceeds pending disbursement

Employee/retiree health benefits and pharmacy management

IT Disaster Recovery and Data Center Services

Lottery – Sports betting

Risks of outsourcing processes -

- Outsourcing processes, in whole or in part, is becoming increasingly common.
- While generally done for efficiency and reduced cost, risk can increase due to loss of control over an entire process.
- Cloud-based, software-as-a-service, outsourcing is increasingly common and presents additional considerations for data security.
- Although tasks or a process has been outsourced, responsibility for those task or processes provided by a service organization cannot be delegated.
- To assess the risks associated with an outsourced service, management needs information about the service organization's controls – hence the SOC report.

What should I do with the SOC report?

Get familiar with the basic components of the report:

- Auditor's report
- Management's description of controls
- Detail of testing performed by auditors
- Management's response to exceptions noted in the testing
- Complementary user-entity controls
- Sub-service organizations identified

✓ What is the time period covered by the report?

✓ What type of SOC report?

✓ For large complex service organizations – are my services included within the scope of this report?

- need a good understanding of the service specifically provided to RI government and how that fits into the overall description of service and controls included within the scope of the SOC report

What should I do with the SOC report?

Is the auditor's report unqualified or unmodified?

- Can have an unqualified report yet exceptions are noted

Are there exceptions noted in the specific testing performed by the auditors?

- usually in a grid form – relatively easy to scan for exceptions
- If an exception is noted – consider relevancy/impact to RI specific contracted services
- Consider if there are compensating controls at either the service organization or within your own operations to mitigate the impact of the reported exception
- Is management's response and corrective action included in the report?
- Consider appropriate follow-up with the vendor/contractor to understand the nature of the exception and what has been done to resolve the issue, prevent re-occurrence

What should I do with the SOC report?

Are user entity controls identified – this helps a user entity understand the parameters and limits of the scope of the report and testing.

- For example, for an EBT benefit process – determination of eligibility for benefits would likely be listed as a user entity control since the EBT processor is only handling the disbursement of benefits.
- Review the user entity controls identified – consider and document applicability.
- When applicable – should prompt consideration of how the user entity controls align with the overall controls for a process or activity

Are sub-service organizations identified ?

- If yes – consider the applicability and whether a separate SOC report exists for the sub-service organization.
- A common sub-service organization is a data center where the application and data is housed – often there will be a separate SOC report covering the data center operations

What should I do with the SOC report?

An important objective is to understand where the service organization's controls begin and end within the overall controls for a given process or activity – understand the boundaries of the coverage of the report.

> ***For example – processing of SNAP benefits – RIBridges determines eligibility for the program and the determination of the benefit amount – the service organization receives information and makes the benefit available through the EBT network and settles food purchases, and maintains individual and aggregate cash settlement data for benefits authorized.***

The SOC report provides you with relevant information and assurances regarding that portion of the controls that our outside of your direct management and oversight.

What should I do with the SOC report?

- Track the availability of SOC reports and obtain and review promptly to be aware of any issues. The reports are typically available on a predictable cycle – consider if there are gaps in coverage.

- Document your review of the SOC report(s) that are relevant to your department/agency's controls. When sub-service organizations are identified and relevant – consider the need to obtain a SOC report for the subservice organization.

- Make your review documentation available to the Office of Accounts and Control (template provided) and the Office of the Auditor General for their audit purposes

User Entity Controls

Complementary User Entity Controls	Related Control Objective(s)
Controls should be established to restrict physical and logical access to authorized personnel for systems sending data to and receiving data from FIS	Control Objective 1 Control Objective 3*
Controls should be established to supervise, manage, and monitor the use of FIS services by user entity personnel. Among the access controls that should be established are the following: • An individual with sufficient authority and accountability is assigned to the security function. • Security Administrator activities are monitored as determined necessary. • Passwords are kept confidential, changed on a regular basis, and in line with user entity policies. • Access to subsystems and sensitive transactions is restricted to authorized individuals. • Procedures to communicate, monitor, and approve security requests are established and followed. • Application-level security provides appropriate segregation of incompatible functions. • Security violations are monitored and investigated as necessary. • Transferred and terminated users are removed completely, accurately, and timely	Control Objective 3*

User Entity Controls

Complementary User Entity Controls	
Controls should be established to monitor and follow up on reported problems or special processing requests.	Control Objective 4
Controls should be established to review, test, and approve requested changes made to production systems and configurations.	Control Objective 5

*This is a complementary control and is required to achieve design and operating effectiveness for this particular control objective.

User Entity Controls

Complementary User Entity Controls	
User access is periodically reviewed and maintained.	Control Objective 3
Controls should be established to notify FIS of changes made to the user entity's authorized technical or administrative contact information in a timely manner.	Control Objective 3*
Controls should be established to review available reports, including evaluating and assessing the information, as appropriate, and taking action if necessary.	Control Objective 4
Controls should be established to provide only properly authorized, complete, and accurate data files to FIS for processing.	Control Objective 4*

Examples of an Exception

Control Objective 1 Controls provide reasonable assurance that physical access to the Technology Center location is restricted to authorized personnel.			
Control Activity	**Control Activity**	**Tests Performed By Service Auditor**	**Results of Testing**
1.6	Physical access of terminated employees is removed within one business day following notification from Human Resources or management	**Inspection:** Inspected the tickets and supporting documentation for a sample of terminated employees during the specified period and verified that each selected terminated employee's physical access was removed within one business day following notification from Human Resources or management	Exceptions noted. The Service Auditor noted that two out of 60 selected terminated employees did not have their access removed within one business day following notification from Human Resources or management.

Example of Management's Response to Testing Exceptions

Control Objective 1 Controls provide reasonable assurance that physical access to the Technology Center Locations is restricted to authorized personnel.		
Control Activity	**Tests Performed By Service Auditor**	**Results of Testing**
Management's Response: Management accepts these findings. For one finding, the PM termination file addressed to the local physical security admin had been overwritten with the AM termination details. Beginning on July 27, 2018, a new termination communication process has been implemented which eliminates this possibility. It was confirmed that the user did not utilize their access following the date of termination. Following the identification of this issue, physical security compared a complete termination listing for the past 19 months with a complete export of the card access system. For any cards still in the system, it was verified that all access had been removed and those cards were deleted from the card access system completely. There is also a procedure in place which removes any physical security permissions which are not used within the past 30 days. This process successfully removed the rights of the user in question. This user held only general building access to a non-data center location. Going forward, the local physical security admin will continue to receive termination files twice daily and remove all privileges considering the date of termination. For the second finding, the termination report was reviewed by the local security officer but the officer failed to remove this one user in question. A senior officer completed a formal review of the prior week terminations and acted on this discrepancy. It was confirmed that the user did not utilize their access following the date of termination. There was a total of four business days between the termination communication and the access removal date. Future discrepancies will log more of the pertinent details and necessary actions will be taken. In like instances, officers will complete re-trainings and disciplinary steps will be taken if they are responsible for reoccurring inaction. This user held only general building access to a non-data center location.		

Office of Accounts and Control - SOC Review and Documentation Process

See review template (handout)

Questions?

Office of the Auditor General

Dennis Hoyle, Auditor General dennis.hoyle@rioag.gov 401.222.2435

Office of Accounts and Control

Margaret Carlson Margaret.Carlson@doa.ri.gov 401.222.2274

Gail LaPoint Gail.LaPoint@doa.ri.gov