Third Party Attestation Reporting (SOC Reports) and Role of Internal Audit

Advisory

February 13, 2014
With You Today

JEFF THOMAS
Partner
Jeff is a Partner in KPMG’s Advisory Services practice in Alberta with over 20 years of experience serving publicly accountable entities, primarily in Western Canada. Jeff is focused on delivering Risk Consulting services to enable decision making, resource allocation and the achievement of organizational objectives. Jeff helps organizations with governance and stewardship, including business processes and controls, compliance with regulations and policy, audit reports on controls over the operation of service providers, IT project review and advice, and information security, privacy and control services.

RAJ DEVADAS
Senior Manager
Raj is a Senior Manager in KPMG’s Internal Audit, Risk and Compliance Practice. He has over 15 years of internal audit and IT audit experience in Information Risk Management, Attestation engagements and IT project risk assessments. He has lead and conducted Numerous Section 5900, Section 5970, Section 9100, Section 5805, Section 5025 and CSAE 3416/SSAE 16 in Canada. An active member of the IIA, Raj is a Certified General Accountant (CGA), Certified Management Accountant (UK), Certified Information Systems Auditor (CISA) and Certified Internal Auditor (CIA).
Contents

- Attestation Reports - Introduction
- Service Organization Control Reports - CSAE 3416/SSAE 16/ISAE 3402
- Role of Internal Audit while Conducting SOC Audits
- Questions
Attestation Reports - Introduction
What are Attest Engagements

- As per PCAOB (AT 101) - Attest engagements are where a certified public accountant in the practice of public accounting is engaged to issue or does issue an examination, a review, or an agreed-upon procedures report on subject matter, or an assertion about the subject matter that is the responsibility of another party.

- The subject matter of an attest engagement may take many forms, including the following:
  - Historical or prospective performance or condition (for example, historical or prospective financial information, performance measurements, and backlog data).
  - Physical characteristics (for example, narrative descriptions, square footage of facilities).
  - Historical events (for example, the price of a market basket of goods on a certain date).
  - Analyses (for example, break-even analyses).
  - Systems and processes (for example, internal control).
  - Behavior (for example, corporate governance, compliance with laws and regulations).
Our Experience - Organizations that use Attestation Reports

From experience we generally see the following organizations require Attest reports:

- **Service providers** are being requested or required to provide **greater transparency about their internal controls environment** to a variety of internal and external stakeholders.

- Business events such as globalization, **increased outsourcing and shared service centre models present new challenges** demanding a greater need for assurance over non-financial reporting areas (Operational, risk and compliance, data privacy, confidentiality) as well as demand for comfort over financial reporting processes for service provider customers and their auditors.

- The **increasing use of cloud computing companies** has created an increasing demand for CPAs to report on nonfinancial reporting controls implemented by cloud computing service providers.

- Use of attestation reports are more prevalent in service organizations, such as those managing information technology, payroll, procurement, where regulatory compliance is required and financial services.
Does your Organization Require an Attestation Engagement?

The response to the four questions below will provide the answer:

1. How do you instill confidence in your various stakeholders about the services you provide?
2. Are your organization's services relied upon by various users/market participants. Does your organization operate in a highly regulated market?
3. Do your customers frequently request information on internal controls or access to audit in accordance to contractual requirements?
4. Are prospective customers routinely inquiring about your internal controls as part of a request for proposal process?
Types of Attestation Reports

- CSAE 3416/SSAE 16 or ISAE 3402 SOC 1 Report - for controls over users’ financial reporting
- SOC 2 Report - based on Specified Trust Principles
- SOC 3 Report - based on Specified Trust Principles
- Section 5025 General Audit Standard
- Section 9100 and 9110 Report - Agreed upon procedures
- Section 5805 Report - Auditors report on financial information other than financial reports
# Comparison Between the Types of Attestation Reports

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of Reporting</td>
<td>Specified procedures and results of testing. No opinion is provided. Auditor only states test results</td>
<td>Audit opinion provides reasonable assurance over the achievement of control objectives, based on the criteria defined with management Assurance report provided to Management or third party</td>
<td>Audit opinion provides reasonable assurance over the achievement of control objectives Type I - Design of controls as at a specified point in time Type II - Design and effectiveness of controls over a specified period of time (SOC 1 and 2 only)</td>
<td>Same as SOC 1</td>
<td>Same as SOC 1</td>
</tr>
<tr>
<td>Report Aspects</td>
<td>No Opinion Criteria used and results of tests performed</td>
<td>Audit Opinion No Management Assertion Control Objectives and Activities Test Procedures and Results</td>
<td>Audit Opinion Management Assertion Description of System &amp; Controls Control Objectives and Activities Tests of Operating Effectiveness (Type II)</td>
<td>Same as SOC 1 except: No Control Objectives (pre-defined criteria)</td>
<td>Same as SOC 1 except: No Control Objectives or Activities (pre-defined criteria) No Type II Reporting</td>
</tr>
<tr>
<td>Management Assertion</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Required by Service Organization</td>
<td>Required by Service Organization</td>
<td>Required by Service Organization</td>
</tr>
</tbody>
</table>
# Comparison Between the Types of Attestation Reports

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicability</td>
<td>Financial processes (not necessarily controls) where only a statement of fact (test result) is required</td>
<td>Reporting for risks and controls where the entity is not a service organization</td>
<td>Financial reporting for risks and controls of a service provider Service providers’ processes used to record, process and report transactions, including supporting technology processes.</td>
<td>Operational controls at a service provider related to any combination of: - Security - Availability - Confidentiality - Processing integrity - Privacy</td>
<td>Same as SOC 2</td>
</tr>
<tr>
<td>Scope</td>
<td>Determined by Stakeholder Pre-determined criteria are used rather than control objectives</td>
<td>Determined by Stakeholder and Auditor to ensure that scope is reasonable for providing an opinion.</td>
<td>Processes impacting financial reporting objectives of user entities.</td>
<td>Defined by service provider Pre-determined criteria are used rather than control objectives</td>
<td>Same as SOC 2</td>
</tr>
<tr>
<td>Report Users</td>
<td>Restricted distribution to specified stakeholders, may include 3rd parties</td>
<td>Restricted distribution to specified stakeholders, may include 3rd parties</td>
<td>User entities and their independent auditors Restricted distribution</td>
<td>Customers and business partners Restricted distribution</td>
<td>Unrestricted use (e.g. online seal)</td>
</tr>
</tbody>
</table>
Discussion on Service Organization Control (SOC) Reports

CSAE3416/
SSAE16/
ISAE 3402
Key Considerations

- SOC reports introduction
- SOC controls audit process
- SOC 1 Report
  - Requirement for management assertion
  - Requirement for subservice organizations
  - Example of audit opinion
  - Control objective, controls and test results - control matrices
- SOC 2 and SOC 3 report
SOC Reports - Introduction

**SOC 1 report based on CSAE 3416**
- Restricted Use
- Type I or Type II report
- Purpose: Reports on Controls over users financial reporting

Reports on controls at a service organization relevant to user entity’s internal control over financial reporting.

**SOC 2 report based on CPA Section 5025**
- Generally a restricted use of the report
- Type I or Type II report
- Purpose: Reports on Controls related to compliance or operations

Trust Services Principles and Criteria Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy.

**SOC 3 report based on CPA Section 5025**
- General Use of report with a Public Seal
- Purpose: Reports on Controls related to compliance or operations
SOC Controls Audit Process

Planning
- Identify services, processes and underlying systems and confirm control objectives
- Understand participants’ and stakeholders’ reliance on organization’s services
- Identify inherent risks in the services

Test of Design and Implementation
- Evaluate organization’s internal control environment, risk assessment and monitoring processes
- Perform process and control walkthroughs
- Review management’s description of controls
- Evaluate the fairness of presentation
- Evaluate the adequacy of the design of the controls

Test of Operating Effectiveness
- Conduct tests of operating effectiveness
- Conduct inventory count and confirmation of ledger balances
- Evaluate exceptions noted in the operating effectiveness of controls

Completion
- Analyse results
- Review and evaluate findings with management
- Form audit opinions
- Communicate with Audit Committee
- Issue deliverables
SOC 1 Report
Components of a SOC Report

1) Management Assertion
2) Audit Opinion
3) Description of the Process
   - Scope of the Report
   - Sub Service Organizations
   - COSO Elements - Control Environment, Risk Management, Information and Communication and Monitoring
   - Description of the Processes
   - User Control Considerations
4) Control Matrices
5) Other Matters - That the organization wishes to communicate with the user of the report which includes BCM/DRP and other controls (this section clearly states that it is unaudited)
Written Management Assertion

- As per the new CSAE 3416, Management has to provide the Service auditor a written Management Assertion.

- Management Assertion covers the following:
  - The description of the system is fairly presented.
  - Suitability of the design of the controls and that they were implemented during report period.
  - Controls were operating effectively (Type 2 examination) throughout the period.

- Management uses monitoring activities (formal and informal) to ensure assertion and control objectives are met.

- The obligation of Management is that they should have a reasonable basis for the assertion.
Assertion - The controls related to the control objectives stated in the description were suitably designed and operated effectively

Risk Assessment

- Service organization management must identify risks that threaten the achievement of the control objectives stated in the description of the system.
- May be formal or informal processes, require ongoing monitoring/updating.
- While preparing for a SOC 1 report, this risk assessment process takes up-front effort.

Basis for Assertion

- Management needs a reasonable basis to provide the assertion.
- There is no requirements on specific procedures to be performed.
- Management may not rely solely on the testing done by the service auditor.
Basis for Management’s Assertion

Organization’s Maturity Relative to Controls
Requirement for Subservice Organizations

The standard allows the Inclusive Method or Carve-out Method:

- Inclusive method - the sub service organization is treated as an extension of the service organization. Sub-service organization controls are tested and it provides an assertion on the relevant controls.

- When carve out occurs the sub service organization is excluded from testing purposes. However Monitoring controls over the subservice organization is tested by service auditor.

Impact to Organization:

- Classify third party relationships.
  - Are they sub-service organizations or vendors?
  - Sub-service organization when the achievement of a control objective relies on the third party, e.g. maintenance of network/cloud services etc.

- For those considered Sub Service Organizations - decide to include or carve out (currently carved-out).

- For the carved out Sub Service Organizations - describe monitoring controls on the report.

- External Auditors will test the monitoring controls as part of the audit.
The Audit opinion covers the following areas:

- **Scope Paragraph** - Description of the system
- **Service Organization Responsibilities** - That the service organization is responsible for:
  - The description of the system
  - Management assertion,
  - Identifying the risks
  - Selecting the criteria/control objectives and the controls
- **Service auditors responsibilities**
- **Inherent limitation** (of the report)
- **Opinion paragraph**
- **Restricted use of the report**

The opinion is generally addressed to the Service Organization.
1. **Control objective**: Controls provide reasonable assurance that changes to the applications, supporting system software and production data are authorized, tested, approved, properly implemented and documented.

<table>
<thead>
<tr>
<th>Control procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1: Policies and standards related to system development are documented and communicated. These include the IT risk policy, the system, development, enhancement and maintenance policy, the <em>Project Management</em> policy and the <em>Change Management</em> policy.</td>
</tr>
<tr>
<td>1-2: A project delivery life cycle framework is established to provide guidance on project activities and deliverables at different project phases.</td>
</tr>
<tr>
<td>1-3: An adequate segregation of duties is in place for application development, change management, technical support, computer operations and security administration.</td>
</tr>
</tbody>
</table>
Control Objective, Control Procedures and Test Results for Type II Report

Change management – application changes

Control Objective #21: Controls provide reasonable assurance that changes to application software are authorized, tested, approved, properly implemented and documented.

<table>
<thead>
<tr>
<th>Description of controls provided by the organisation</th>
<th>Test of effectiveness</th>
<th>Test results</th>
</tr>
</thead>
<tbody>
<tr>
<td>21-1: Standards, procedures and responsibilities for applications change management are documented in the change management policy.</td>
<td>Inspected the change management policy to determine that the standards, procedures and responsibilities for application changes were documented, appropriate, communicated and current.</td>
<td>No relevant exceptions noted.</td>
</tr>
<tr>
<td>21-2: Separate environments are maintained for development, SIT, UAT and production.</td>
<td>Inspected network diagrams for evidence of separation of development, UAT and production.</td>
<td>No relevant exceptions noted.</td>
</tr>
</tbody>
</table>
SOC 2 & 3 Report - Options

- Each principle and criteria (except Privacy) is organized into four broad areas

- Privacy criteria testing is based on Generally Accepted Privacy Principles (GAPP) 10 principles
SOC3<sup>SM</sup> Report Distribution

**SOC3<sup>SM</sup> Report Distribution Options Include:**

- Selective distribution (e.g. hard copy report)
- Limited distribution through restricted portion of client’s website
- General availability through linkage to the SOC Seal on the client’s web site
## SOC2 Report Structure - Contrasted with SOC1

### SOC1

**Control Objective 1: Xxxxxxxxx**

<table>
<thead>
<tr>
<th>Control</th>
<th>Test Procedures</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxx</td>
<td>■ Xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td></td>
<td>■ Xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td></td>
<td>■ ....</td>
<td>....</td>
</tr>
</tbody>
</table>

**Control Objective 2: Xxxxxxxxx**

<table>
<thead>
<tr>
<th>Control</th>
<th>Test Procedures</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td></td>
<td>■ ....</td>
<td>....</td>
</tr>
</tbody>
</table>

### SOC2

**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.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Test Procedures</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxx</td>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td>xxxxx</td>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ....</td>
<td>....</td>
</tr>
</tbody>
</table>

2.0 **Communications:** The entity communicates its defined system security policies to responsible parties and authorized users.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Control</th>
<th>Test Procedures</th>
<th>Results of Tests</th>
</tr>
</thead>
<tbody>
<tr>
<td>xxxxx</td>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td>xxxxx</td>
<td>xxxxx</td>
<td>■ xxxxx</td>
<td>xxxxx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ ....</td>
<td>....</td>
</tr>
</tbody>
</table>

Deciding on an Applicable SOC Report

**SOC Report Decision Tree**

- **CSAE3416 SOC 1 report**
- **SOC 2 or SOC 3 report**
- **SOC 2 report**

**Q1**: Will the report be used by your customers to evaluate controls related to financial reporting or SOX 404 key controls?
- Yes → **CSAE3416 SOC 1 report**
- No → Do your customers need a report on controls related to system security, availability, processing integrity, confidentiality and/or privacy in order to perform proper oversight or vendor management activities?
  - Yes → **SOC 2 or SOC 3 report**
  - No → Do your customers have the need to review a detailed description of your control environment, the tests performed by the service auditor, and the results of those tests?
    - Yes → **SOC 2 report**
    - No → **SOC 3 Report**
Role of Internal Audit in SOC Audits
Use of Internal Audit - Does the regulator permit it?

- The regulations permit external auditors to use Internal audit’s assistance to conduct the audit.

- Using Internal Audit for SOC report testing would result in it being disclosed:
  - As introductory material to the description of tests of controls.
  - Attributing certain tests to internal audit.

- Two methods of “assistance from internal audit”:
  - Use of the work of internal audit.
  - Direct assistance mode - IA work undergoes a level of direction, review, and supervision that is similar to that of work performed by the service auditor's staff. The auditor should assess the internal auditors' competence and objectivity and supervise, review, evaluate, and test the work performed by internal auditors to the extent appropriate in the circumstances.

- The extent of using the work of the internal audit is a matter of professional judgment (taking into account the nature and scope of the work performed, significance of the work etc.)
Coordinating Testing with the Internal Audit Function

If the Service auditor determines that Internal audit work is going to be used, the following is performed:

- Review the **internal audit function's audit plan** as a basis for determining whether the internal audit function's procedures may be coordinated with the service auditor's procedures.

- **Meet** with the internal audit function to:
  - Understand the role of the internal audit function.
  - Management's directives to the internal audit function.

- **Evaluate and perform procedures** on that work to determine its adequacy (re-performance). Factors considered include:
  - Internal audit function members have adequate technical training and proficiency.
  - The work was properly supervised, reviewed, and documented.
  - Sufficient appropriate evidence has been obtained to draw reasonable conclusions.
  - Conclusions reached are appropriate in the circumstances.
  - Any deviations or unusual matters disclosed.
## Advantages of Using Internal Audits in SOC Audits

<table>
<thead>
<tr>
<th>Advantages</th>
<th>Organization</th>
<th>External Auditors</th>
<th>Internal Auditors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Identification</strong></td>
<td>Focus is on key controls</td>
<td>Review of IA reports identifies risk in the organization</td>
<td>Conducting risk based audits as against process audits</td>
</tr>
<tr>
<td><strong>Effort and Cost</strong></td>
<td>Using IA results in lower cost to the organization</td>
<td>Effort is lower since Internal audit services are leveraged</td>
<td>Internal Audit plan and coverage is achieved for high risk processes</td>
</tr>
<tr>
<td><strong>Audit Process</strong></td>
<td>Effective audits are conducted - different approach and focused audits</td>
<td>Internal audit provides business process knowledge and understanding</td>
<td>External auditors review Internal auditors work resulting in better documentation and audits</td>
</tr>
<tr>
<td><strong>Time</strong></td>
<td>Audits are focused resulting in reduced client face time and audit timeframe</td>
<td>Reduced efforts leads to reduced time requirements to complete the audit</td>
<td>Focus is to complete the SOC audit in scheduled timeframe</td>
</tr>
</tbody>
</table>
Questions?
## Contacts

<table>
<thead>
<tr>
<th>Jeff Thomas</th>
<th>Raj Devadas</th>
</tr>
</thead>
<tbody>
<tr>
<td>403.691.8012</td>
<td>403.691.8105</td>
</tr>
<tr>
<td><a href="mailto:jwthomas@kpmg.ca">jwthomas@kpmg.ca</a></td>
<td><a href="mailto:rdevadas@kpmg.ca">rdevadas@kpmg.ca</a></td>
</tr>
</tbody>
</table>

KPMG LLP  
Bow Valley Square II  
Suite 3100, 205 - 5th Avenue SW  
Calgary, AB  T2P 4B9