www.pwc.com/ca

Third Party Risk Management:

Governing your third-party relationships

May 20, 2015

Canadian Insurance Accountants Association

pwc

Introductions

Jennifer A. Johnson
PwC Tower
18 York Street, Suite 2600
Toronto, ON M5J 0B2
T: +1 (416) 947 8966
F: +1 (416) 814 3215
j.a.johnson@ca.pwc.com

Jennifer A. Johnson
Partner, Risk Assurance Services

Gus Leite
PwC Tower
18 York Street, Suite 2600
Toronto, ON M5J 0B2
T: +1 (416) 815 5265
M: +1 (416) 419 5190
gustavo.leite@ca.pwc.com

Gus Leite
Director, Risk Assurance Services

“You can delegate an activity, but *not* the accompanying ultimate responsibility”

Session topics

1. Why focus on Third Party Risk Management (TPRM)?
2. Critical elements of a robust TPRM framework
3. Governing your third-party relationships
4. Understanding & leveraging Service Organization Controls (SOC) reporting
5. Q&A

Why focus on TPRM?

1

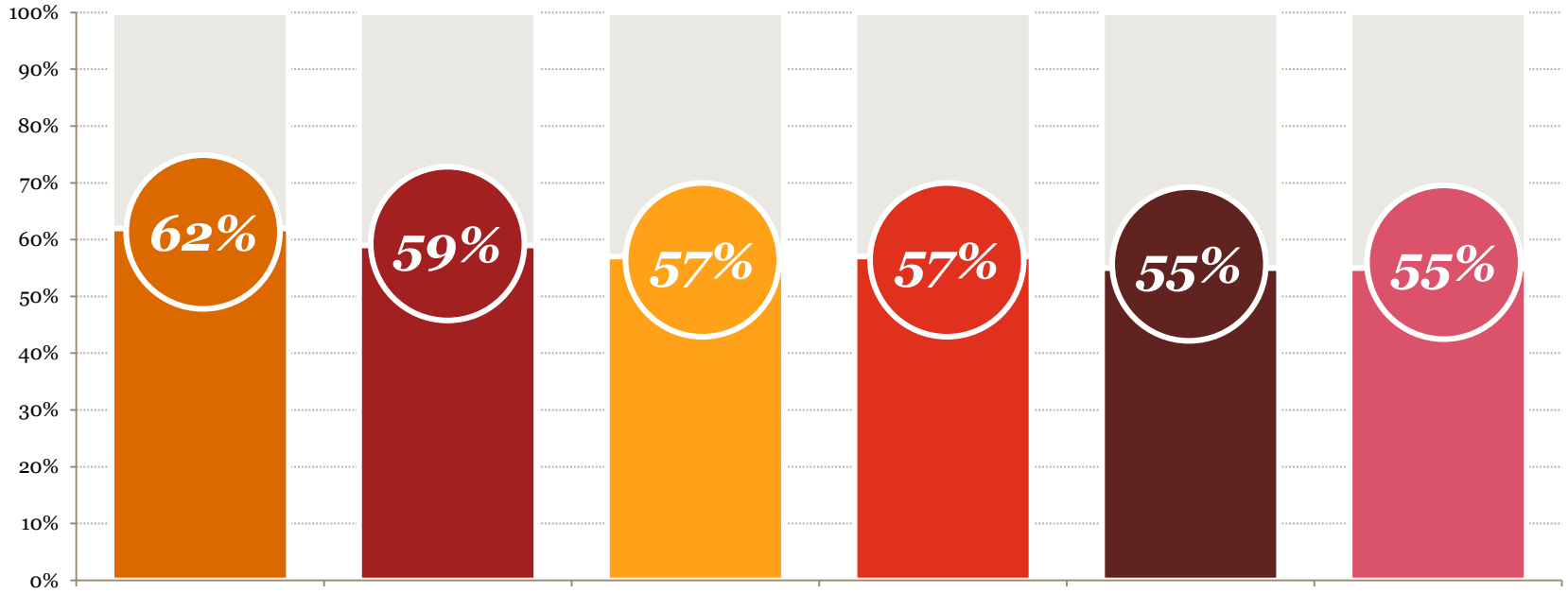
RECENT HEADLINES

- **Bell Canada** announces that a cyber attack on a 3rd-party supplier compromised the confidential account information of more than 22,000 of its small business customers. *The Globe and Mail, Feb 2014*
- Hackers successfully stole prepaid debit card information from the Indian and US-based third-party vendors of several large multi-national credit card institutions, **fraudulently withdrawing $45M from ATMs worldwide**. *Wall Street Journal*, May 2013
- Compromises attributed to **third parties with trusted access** increases while due diligence weakens – *PwC GSISS* 2014
  - 55% have security baselines for external partners, suppliers, and vendors (60% in 2013).
  - 50% perform risk assessments on third-party vendors (53% in 2013).
- Recent Ponemon Institute surveys reveal that unsecure third parties including cloud providers are seen as one of the top three threats to an organization. **41% of the companies surveyed experienced a data breach caused by a third party**.

** Symantec and Ponemon Institute, "2013 Cost of Data Breach Study United States," May 2013*

Rising third-party risks

Key gaps in third-party security – PwC GSISS 2014



Established security / baselines/ standards for external partners/ customers/ suppliers/ vendors

Require third-parties (including outsourcing vendors) to comply with our privacy policies

Incident response-process to report and handle breaches to third-parties that handle data

Inventory of all third-parties that handle personal data of employees or customers and/or financial data

Conduct compliance audits of third-parties that handle personal data of employees or customers and/or financial data

Risk assessment on third-party vendors

Renewed regulator focus

PwC GSISS 2014

Rising third-party risks

*Only 34% of financial services respondents say they have **assessed the security of third-party outsourcers over the past 12 months**.*

*Roughly the same number (33%) report that they began **monitoring fourth-party relationships** over the past year.*

Office of the Superintendent of Financial Institutions Canada | Bureau du surintendant des institutions financières Canada

Guideline

Subject: **Outsourcing of Business Activities, Functions and Processes**

Category: **Prudential Limits and Restrictions**

No: **B-10** **Date:** **May 2001**
Revised: **December 2003**
Revised: **March 2009**[1]

1. Introduction

Financial institutions outsource business activities, functions and processes to meet the challenges of technological innovation, increased specialization, cost control, and heightened competition. However, outsourcing can increase an institution's dependence on third parties, which may increase its risk profile. Many financial sector regulators have responded by introducing guidance related to the management of outsourcing risks.

This Guideline sets out OSFI's expectations for federally regulated entities (FREs) that outsource, or contemplate outsourcing, one or more of their business activities to a service provider. These expectations should be considered prudent practices, procedures or standards that should be applied according to the characteristics of the outsourcing arrangement and the circumstances of the FRE.

FREs have the flexibility to configure their operations in the way most suited to achieving their corporate objectives. However, this Guideline operates on the premise that FREs retain ultimate accountability for all outsourced activities. Furthermore, OSFI's supervisory powers should not be constrained, irrespective of whether an activity is conducted in-house, outsourced, or otherwise obtained from a third party.

What issues are companies facing in this area?

Market drivers

- Substantial reliance on third parties
- Vendor sourcing decisions that often overlook key risks
- Incomplete populations of vendors or vendors with sensitive data
- Inconsistent risk assessment and review practices across organizations
- Complexities in managing third party risk, such as:
  - Identifying what risks really matter
  - Selecting which third parties to review
  - Taking effective action when an issue is found
  - Identifying when your vendor subcontracts to others

Industry/Company-specific triggers

- Regulatory changes
- Negative results from internal or regulatory reviews
- Vendor breach internally or at a competitor

Critical elements of a robust TPRM framework

2

What is Third Party Risk Management?

Focused on understanding and managing risks associated with 3rd parties that you do business with

Comprehensive in coverage of all types of third party relationships

Holistic in its consideration of a full spectrum of risks

TPRM program foundational elements

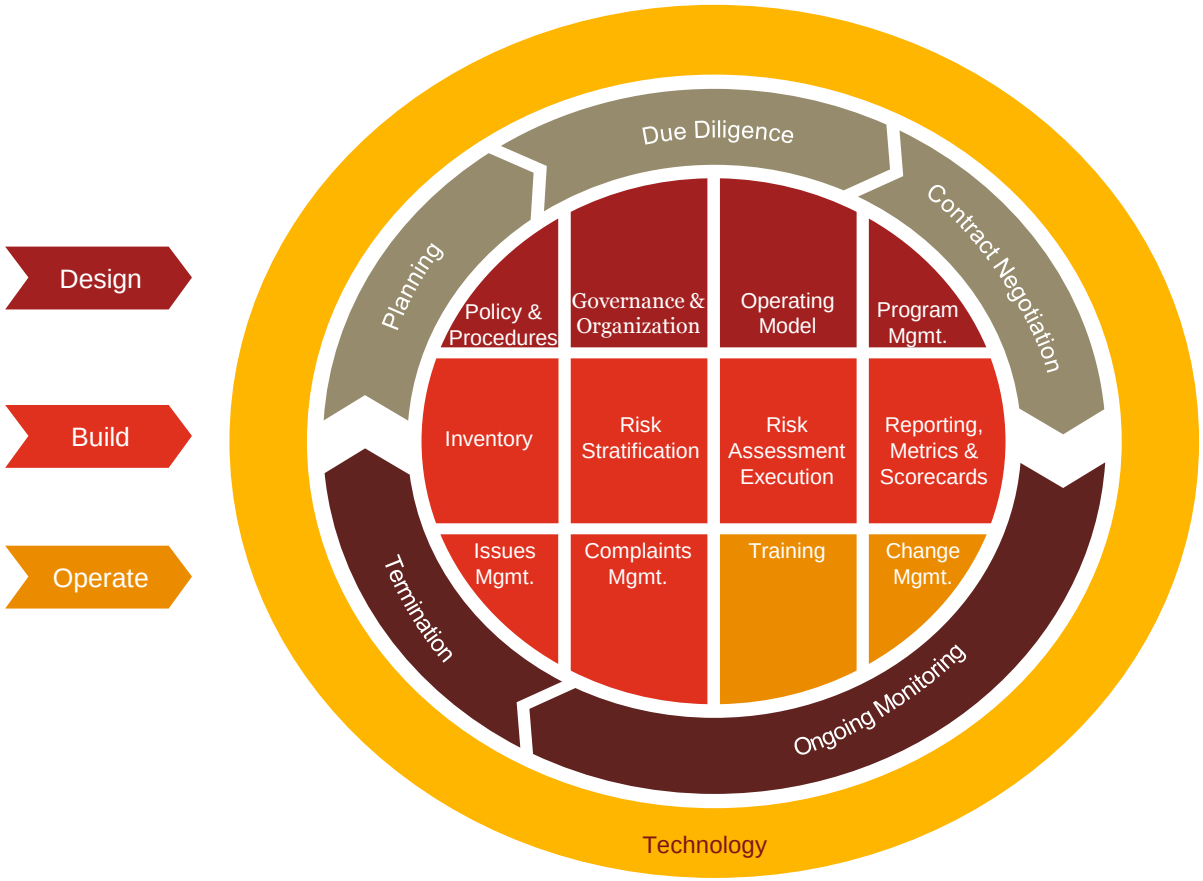
- Vendor Management office
- Operational risk governance body
- Critical Vendor oversight
- Centralized Vendor complaint management support

- Know-your-counterparty/ due diligence
- Standard operational risk methodologies and defined risk levels
- Standard controls effectiveness assessment methodology
- Escalation, exception, and exemption processes
- Customer complaint handling

- Linkages between contracting and payables/general ledger
- Comprehensive contracts management system and contract data
- Well defined and maintained vendor repositories (vendor master, etc.)
- Vendor/ vendor usage data
- Strong organizational and employee data for identifying vendor linkages across the organization
- Issues and incidents repositories to track vendor issues
- Recovery and resiliency – back-up of key/"critical" vendors
- Integrated complaint management system for monitoring and reporting

Third Party Risk Management (TPRM) framework

The PwC Third Party Risk Management Program Framework



Pre-contract

Post-contract

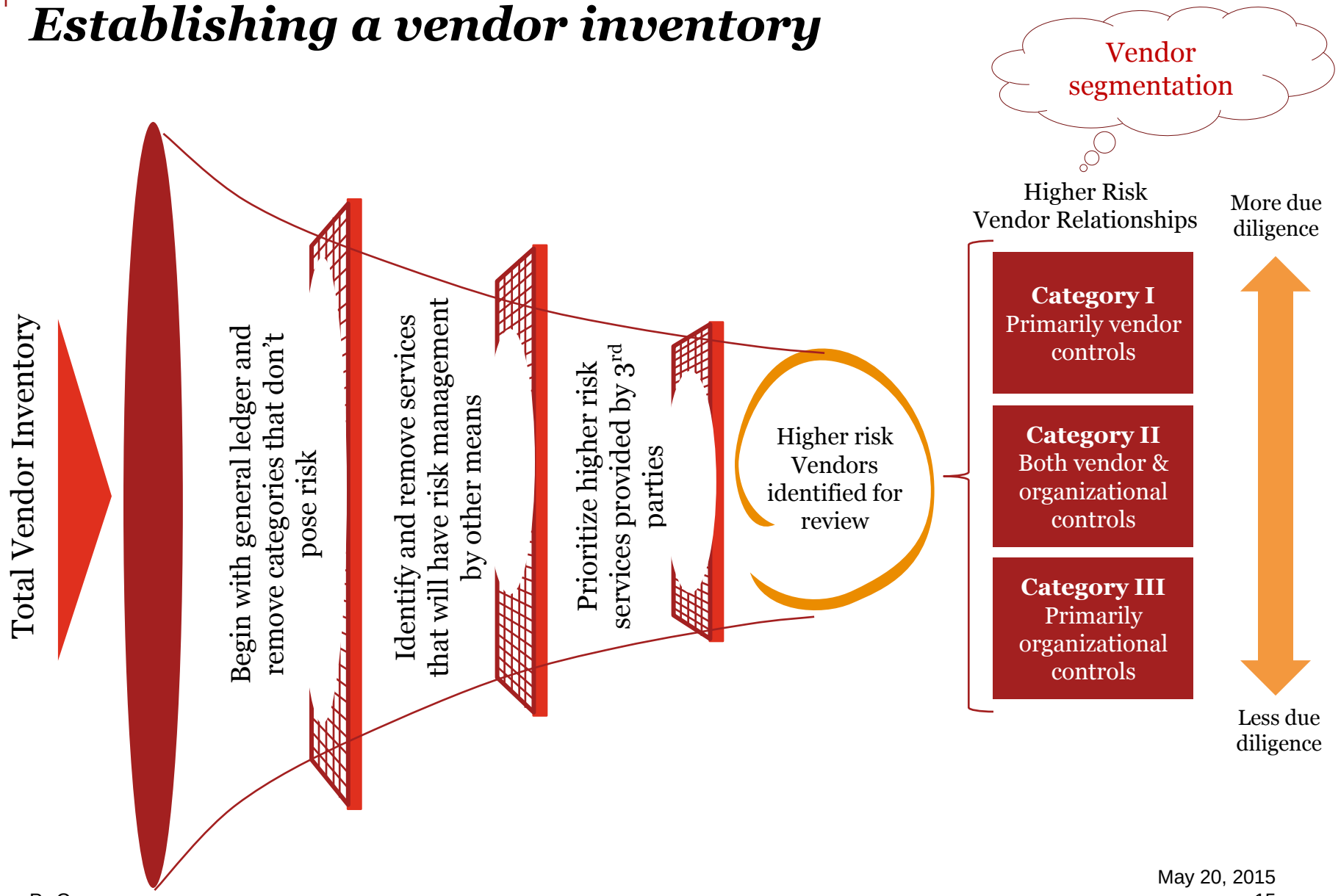
Risk Considerations

- Reputational
- Operational Competency
- Financial
- Business Continuity and Resiliency
- Country
- Physical Security
- Subcontractor
- Information Security & Privacy
- Technology
- Compliance

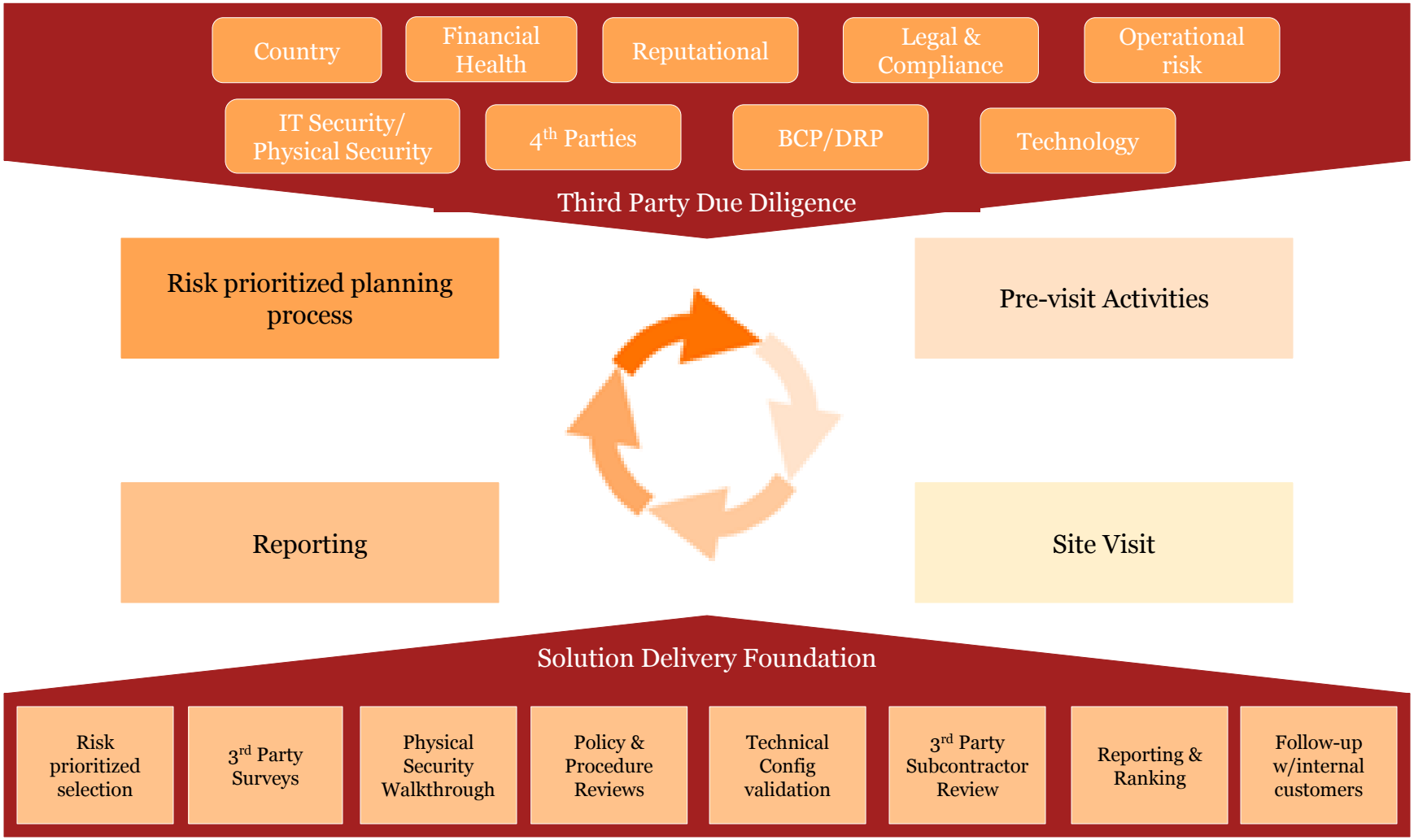
Governing your third-party relationships

3

Establishing a vendor inventory

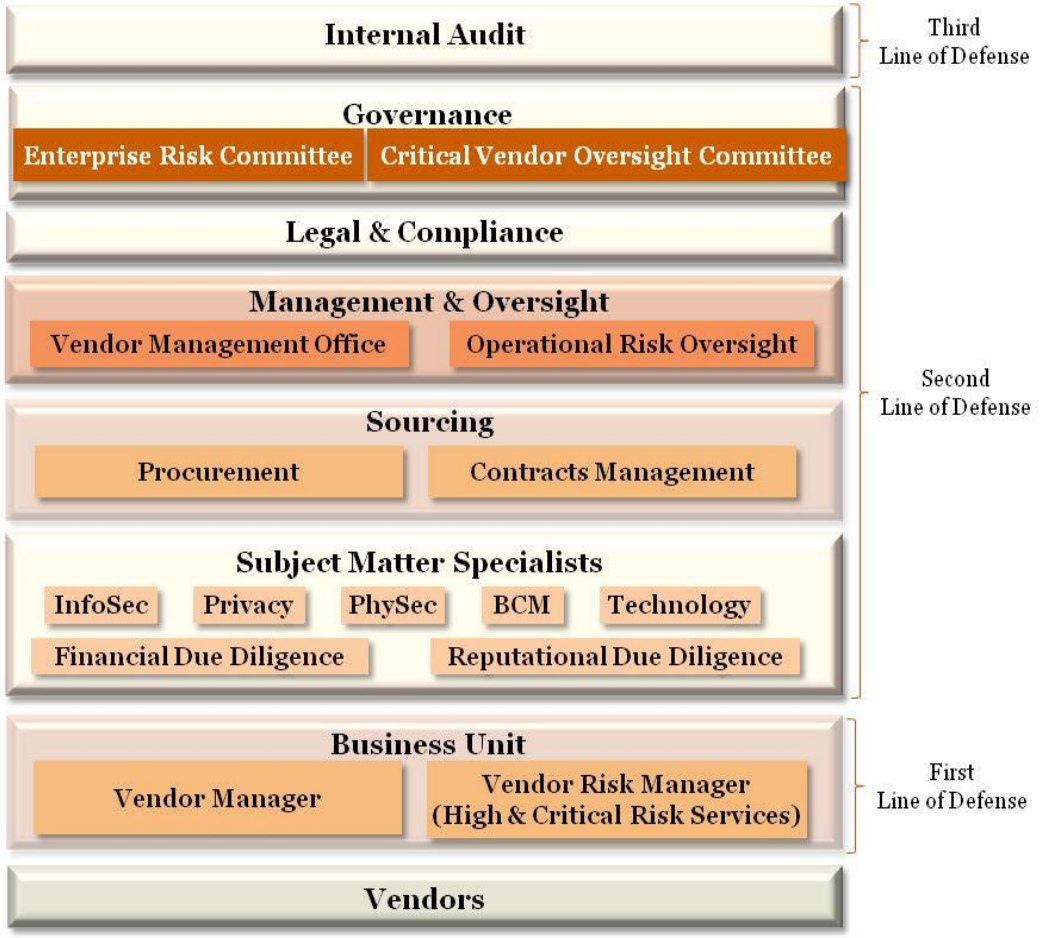


TPRM due diligence approach

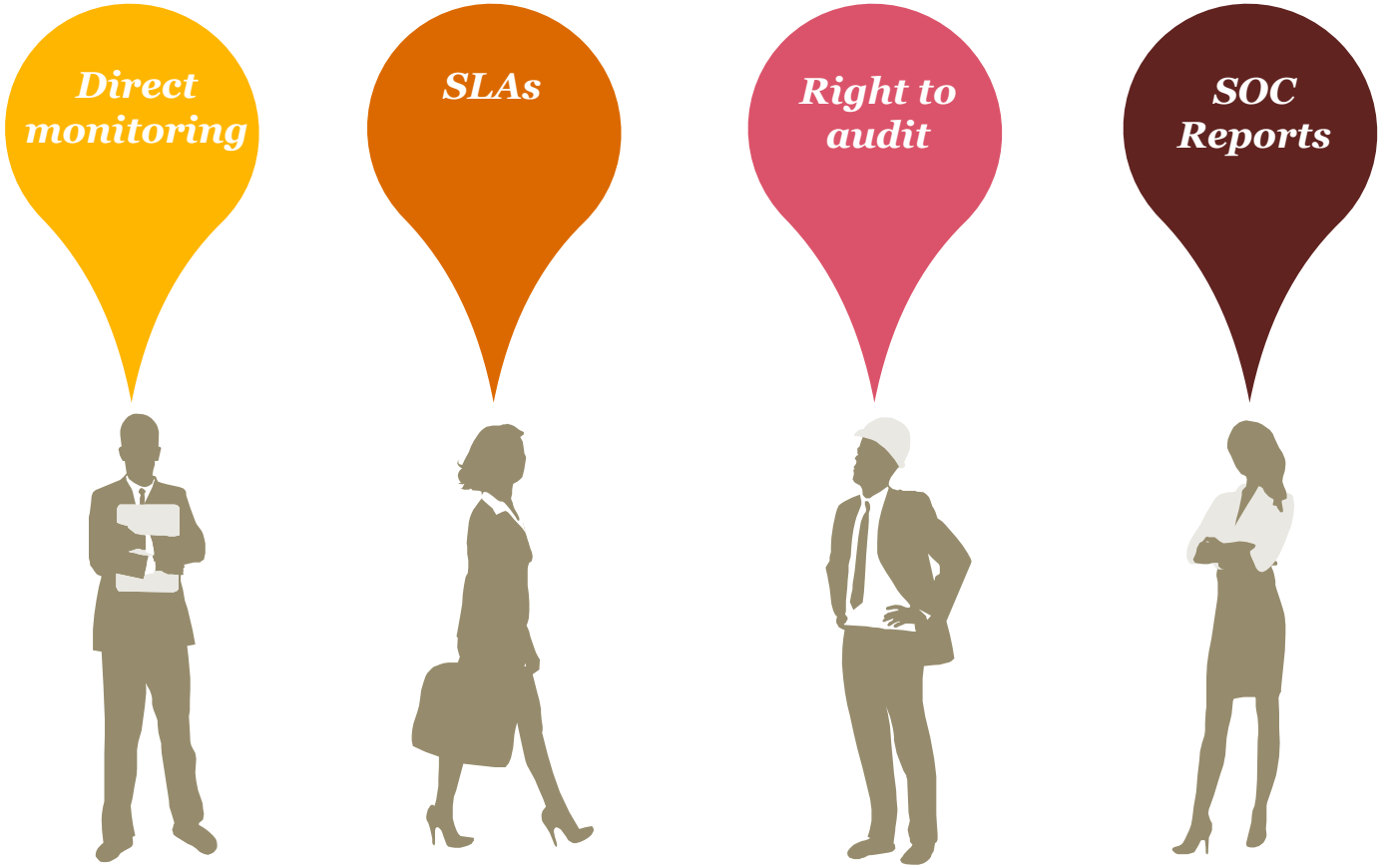


Ongoing TPRM governance model

- A strong governance model is a critical success factor in any TPRM.
- Each “line of defense” plays an important role in ensuring vendor processes and performance meets management’s needs, expectations and contractual requirements.
- Vendors may play an important role in delivery of your services or functioning of your business – however, you retain accountability to your customers/clients.



Approaches to governing third-parties

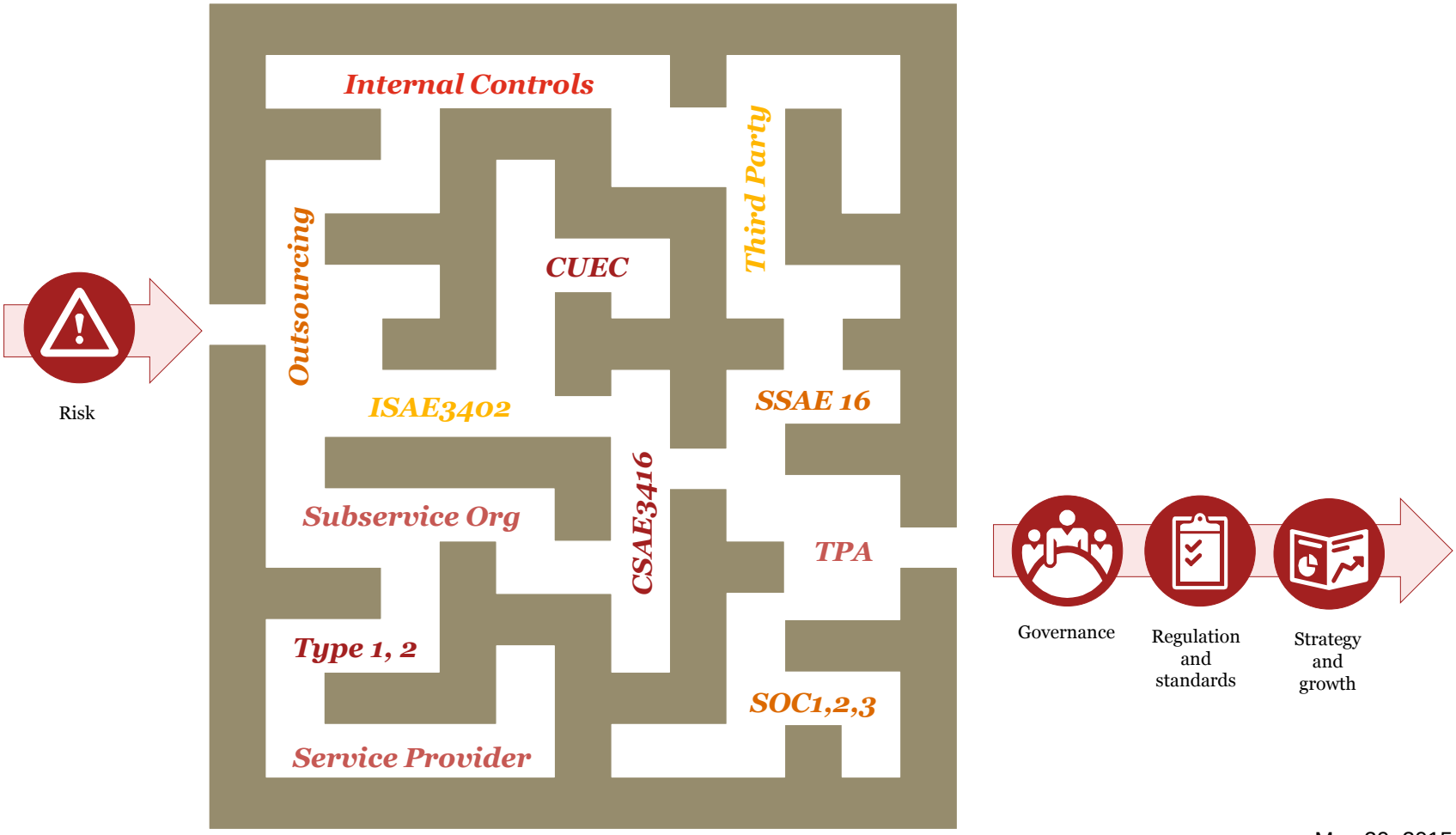


Often we see a combination of these approaches being used

Understanding & leveraging SOC Reporting

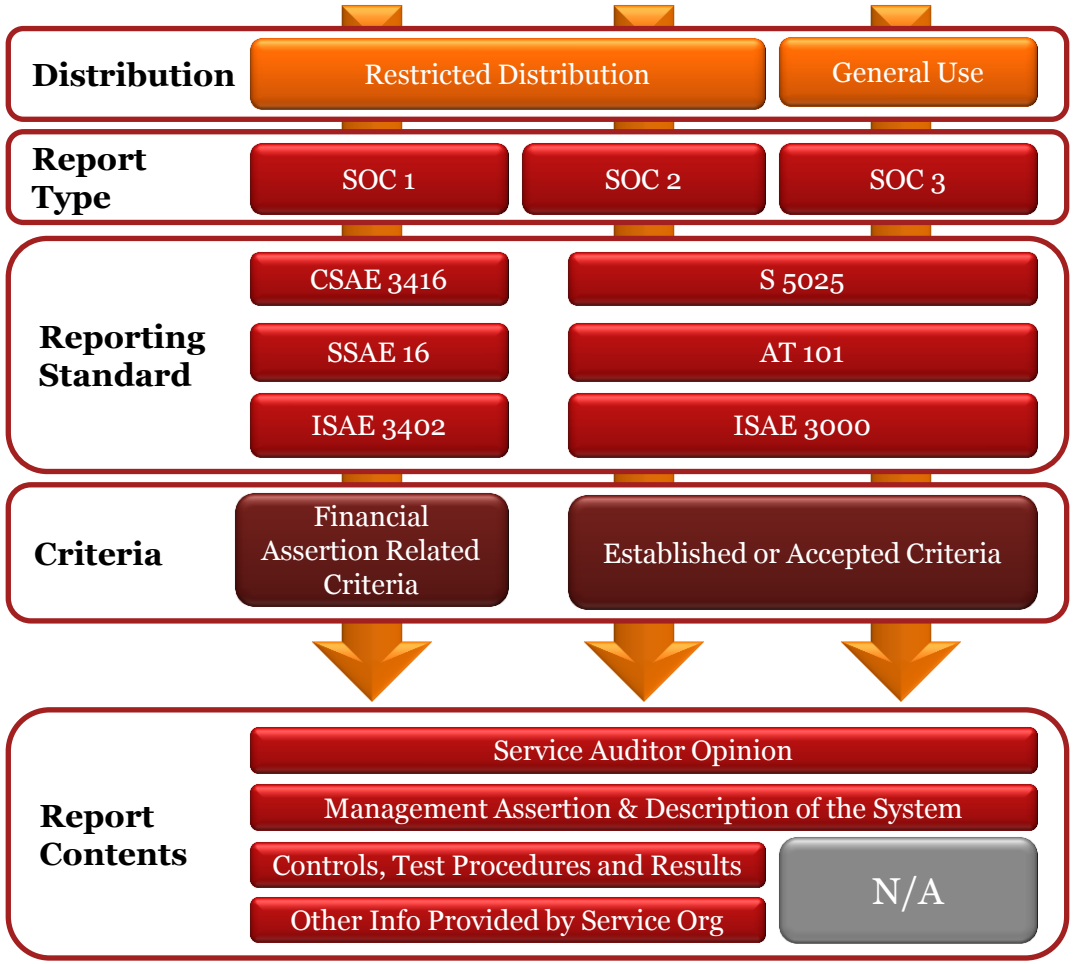
4

SOC Lingo


Internal Controls
Third Party
Outsourcing
CUEC
ISAE3402
SSAE 16
CSAE3416
Subservice Org
TPA
Type 1, 2
SOC1,2,3
Service Provider
Risk
Governance
Regulation and standards
Strategy and growth

What is SOC reporting?

SOC reporting Options



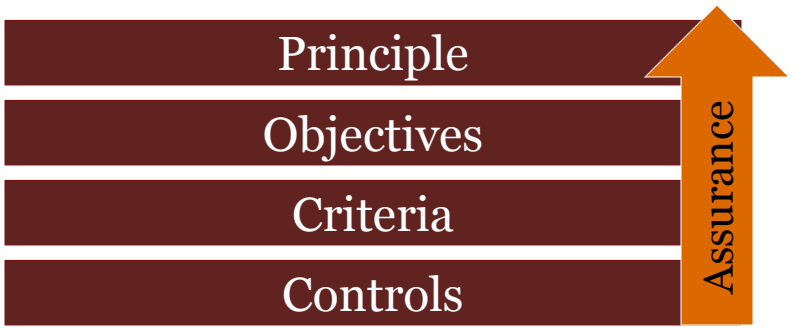
PwC insights:

- We have noted a rise in controls assurance reporting requests over nonfinancial reporting risks such as operational and compliance risks.
- We have noted several organizations that rely on service providers requesting both SOC 1 and SOC 2 reports to obtain broader coverage over financial, operational and compliance risks.
- We have noted a number of financial institutions enhancing their OSFI B10 compliance efforts which have driven or contributed to increased demands for SOC 2 & 3 reporting.

What is SOC 2 & 3?

- Defines **5 principles** as follows:
  1. Security (Common),
  2. Availability,
  3. Confidentiality,
  4. Processing Integrity, and
  5. Privacy.
- Each principle contains **4 objectives** of: policies, communications, procedures, and monitoring.
- Under each objective specific criteria are defined > **Each criteria must be achieved in order to achieve the principle.**

- **Illustrative controls** are provided that align to each criteria and can be used as a guide in determining which controls satisfy each criteria and in turn the principle.
- Once a principle is deemed in-scope **all objectives and criteria must be satisfied** to render an unqualified (clean) opinion on that principle.



Comparison of SOC & related reporting options

Attributes	SOC 1 CSAE 3416 / SSAE16	SOC 2 & SOC 3 (Trust Services)	Agreed Upon Procedures (S9100 / S9110)	General Attest (S5025, ISAE 3000)
Limitations on type of System/ Process?	Yes - Systems that process transactions significant to customers' financial statements	No - Any system	No - Any system or process	No - Any system or process
Scope Limitations (Exclusions)?	Yes - Privacy, disaster recovery/ business continuity	None - as long as they relate to system reliability	None	None
Established Control Objectives/ Principles	No – service organization has flexibility in selecting and defining the control objectives	Yes - Principles and criteria are specified in the framework (Security, Availability, Confidentiality, Integrity, Privacy)	No – controls can be leveraged from any other existing standard or crafted for the review	No – can be aligned with control objectives and/or principles from SOC1-3 or custom/tailored framework, if agreed with report users
Established (Illustrative) Control Activities	No – service auditor applies professional judgment to determine controls necessary to achieve a control objective	Yes – Illustrative controls are provided for each Principle & Criteria	No – controls & tests are specified by the service organization and/or the user organization	See above.
Sample sizes disclosed in report?	No, except for when exceptions are being reported	No, except for when exceptions are being reported in SOC 2	Yes, required	No, except for when exceptions are being reported
Auditor's Opinion provided?	Yes	Yes	No	Yes
Report distribution restricted?	Yes - Limited distribution to existing customers and their auditors	SOC2 – Limited distribution to existing and prospective customers SOC3 - Unrestricted distribution	Yes – Limited distribution to existing customers and their auditors	Depends upon criteria selected for use

Using a SOC report – key considerations

- ***SOC reports are an attestation – not a certification***
- ***It requires evaluation of scope and results***

Q&A