cutting through complexity

IT Attestation in the Cloud Era

The need for increased assurance over outsourced operations/ controls

April 2013

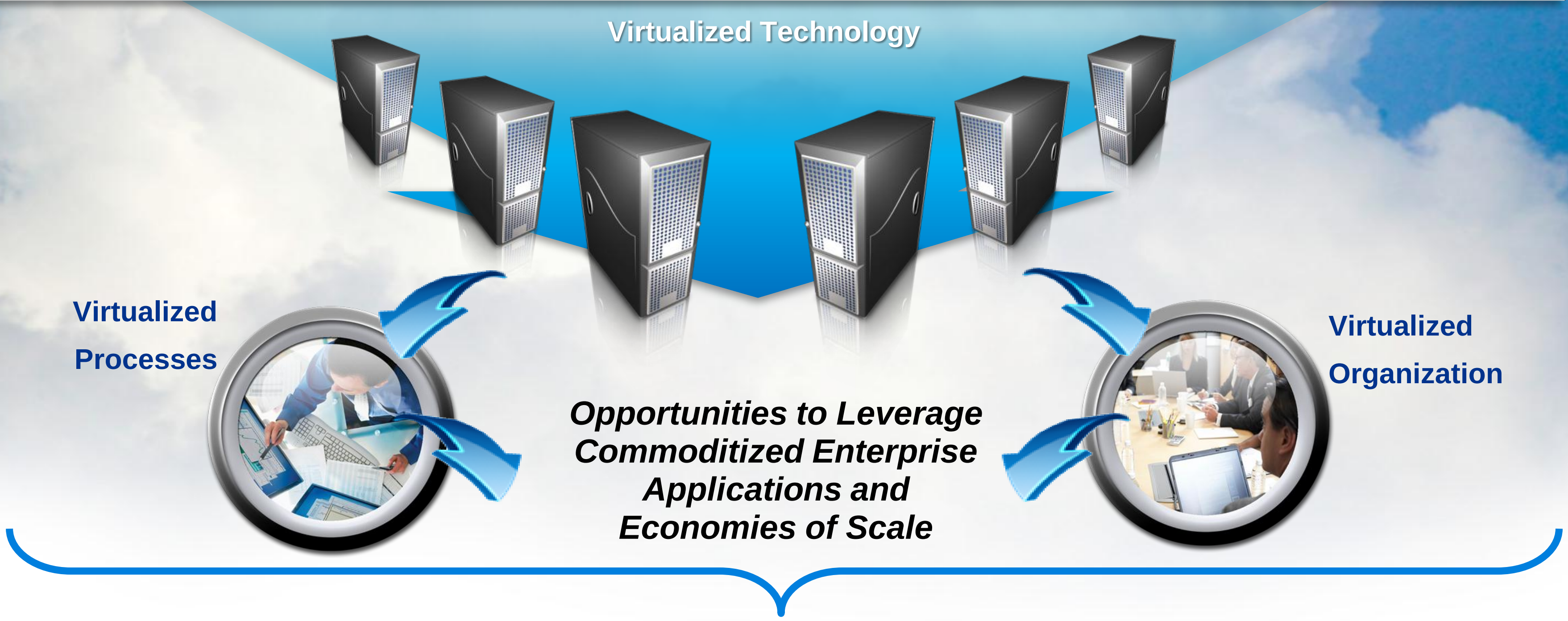
Symeon Kalamatianos M.Sc., CISA, CISM
Senior Manager, IT Risk Consulting

Contents

- Introduction
- SOC Assurance Reporting – Overview & Market Trends
- Effectively using SOC reports
- Conclusion
- Q/A

Cloud Impact on Business

Cloud Environment = Internet-based data access & exchange + Internet-based access to low cost computing & applications



Virtualized Technology

Virtualized Processes

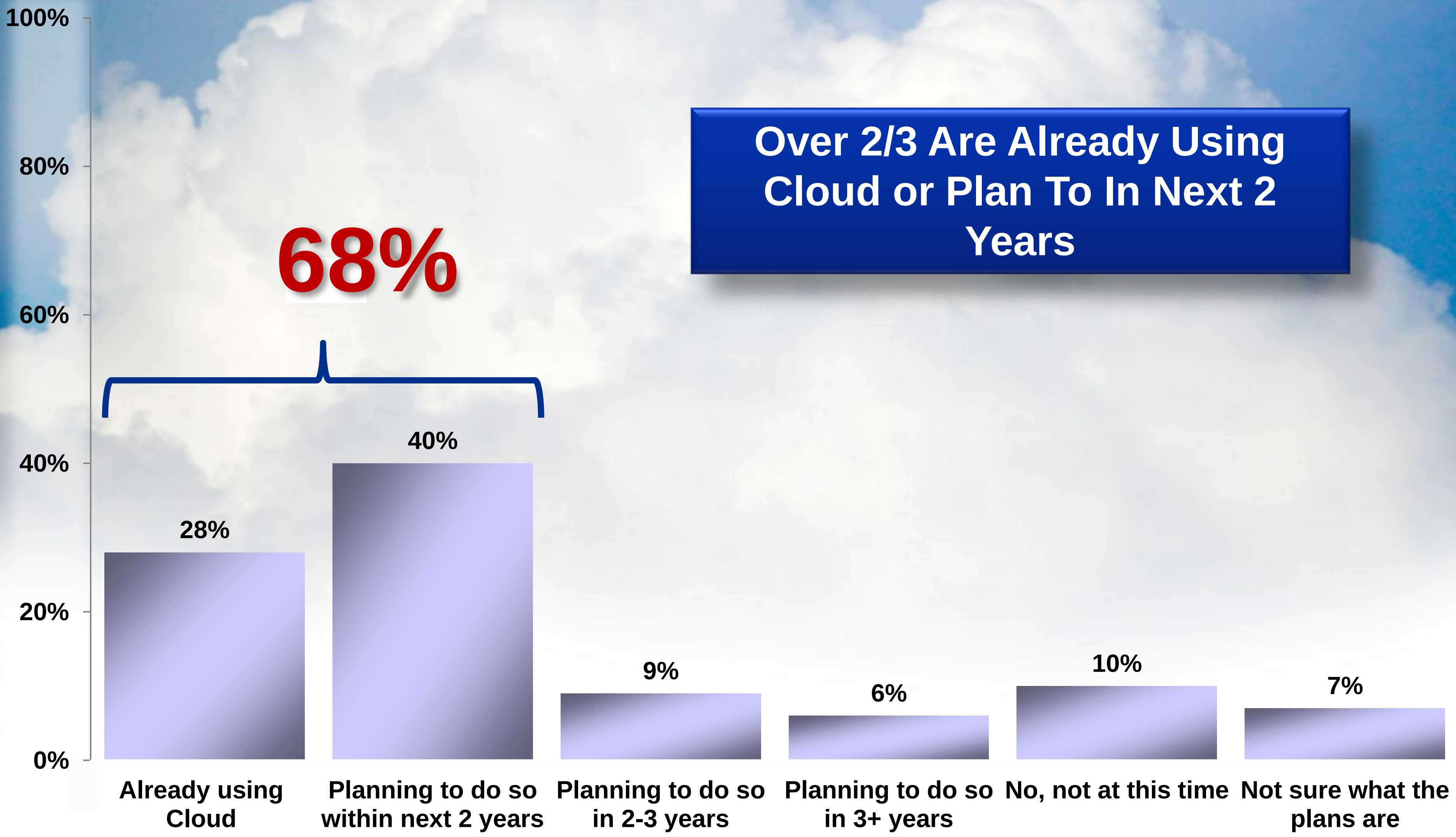
Virtualized Organization

Opportunities to Leverage Commoditized Enterprise Applications and Economies of Scale

Virtualized Business Models

- Speed to Market
- Improve Working Capital
- Reduce Invested Capital
- Reduce Cost of Goods Sold
- Reduce SG&A

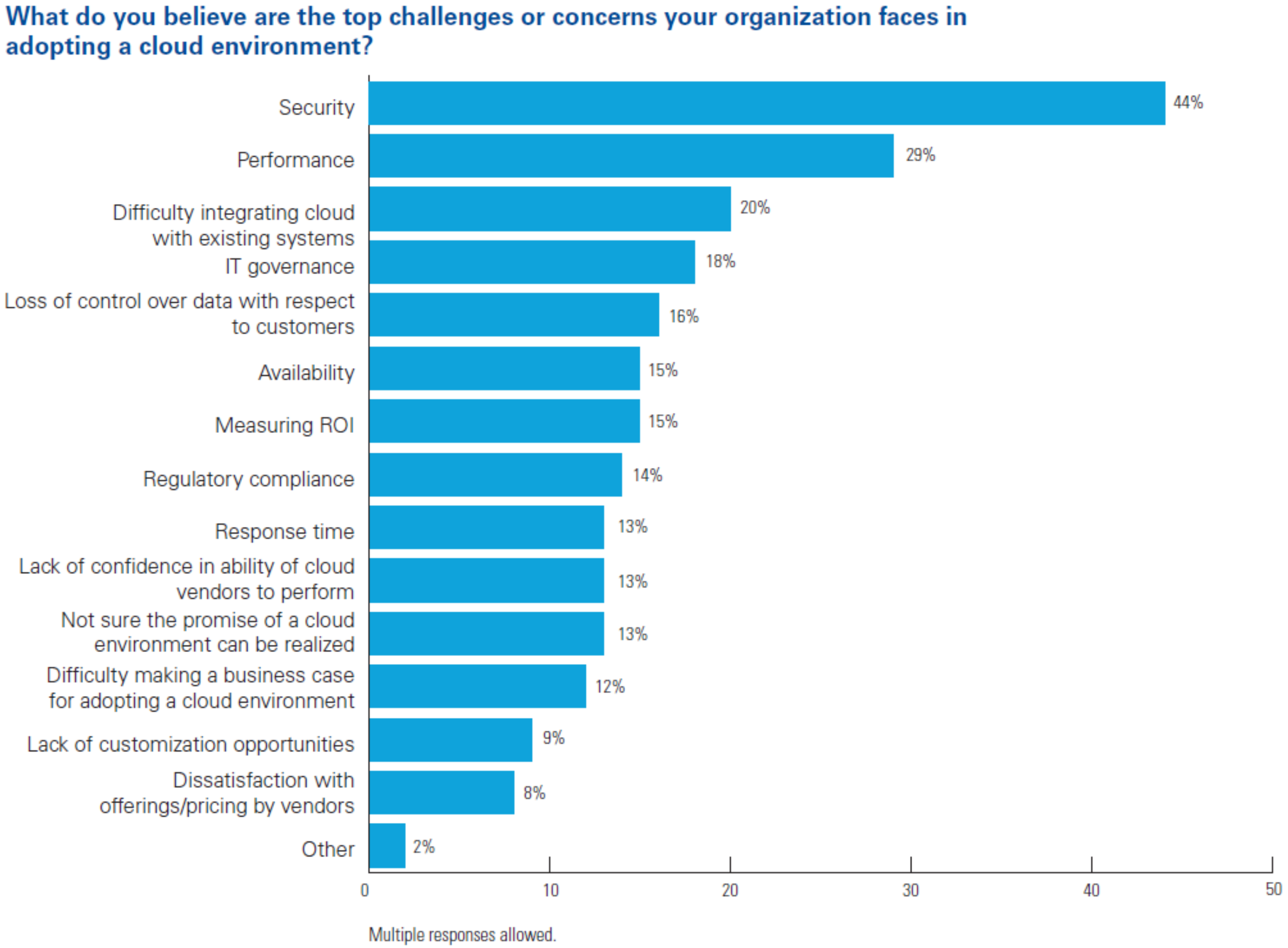
KPMG Recent Survey



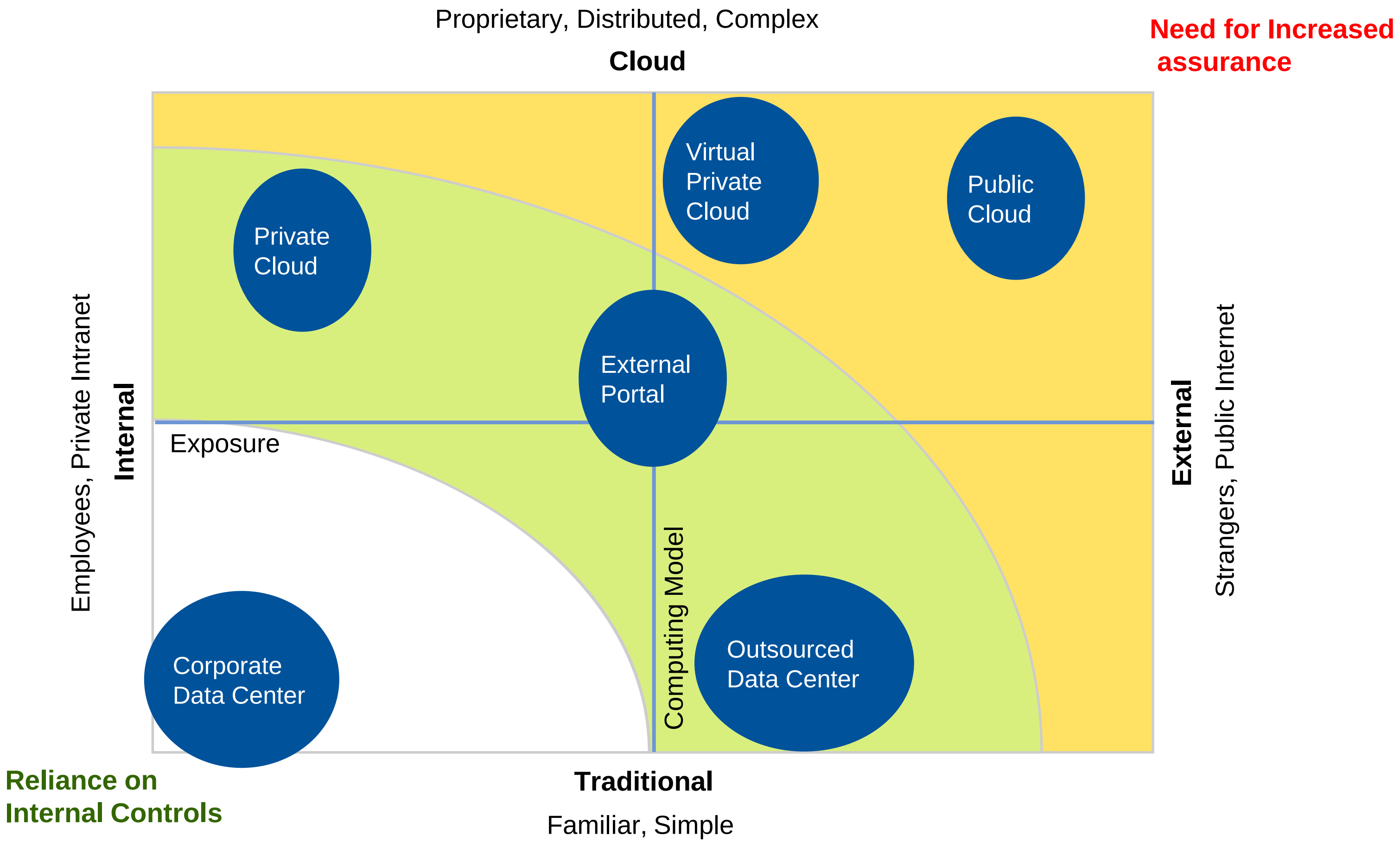
Over 2/3 Are Already Using Cloud or Plan To In Next 2 Years

Key Security Challenges

Security has been the greatest concern surrounding Cloud Adoption at enterprises



Complexity and Exposure define assurance model



Service Organization Control Assurance Reporting – Overview and Market Trends

Service Organization Control (SOC) Assurance Reporting

Scope/Focus	Report	Summary	Applicability
Internal Control Over Financial Reporting (ICOFR)	**ISAE3402 / SOC1***	Detailed report for users and their auditors	- 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.
Operational Controls	**ISAE3000/ SOC2^{SM}**	Detailed report for user organizations, their auditors, and specified parties	- Focused on Trust Services Principles: - Security - Availability - Confidentiality - Processing Integrity and/or - Privacy. - Applicable to a broader variety of systems.
	ISAE3000 / SOC3^{SM}**	Short report that can be more generally distributed, with the option of displaying a web site seal	

**** Sometimes also referred to as an SSAE 16, AT 801***

***** Sometimes also referred to as a SysTrust, WebTrust, or Trust Services report***

Type 1 and Type 2 Reports

- Point in time reports (Type 1) reports cover the suitability of design of controls as of a point in time. The Type I report is a snapshot in time.
- Period of time (Type 2) reports cover the suitability of design and operating effectiveness of controls over a period of time, typically 6 or 12 months.
- For example, a service organization providing a new service might start by completing an initial SOC2 Type 1 examination and then complete recurring SOC2 Type 2 examinations.

Generally, when talking about a service organization control report, a Type II report is meant. A Type I report should be seen as an informative report.

Contrasting SOC2/SOC3 and SOC1 Report Scope

Attribute	SOC2/SOC3	SOC1
Required Focus	• Operational Controls	• ICOFR
Defined Scope of System	• Infrastructure • Software • Procedures • People • Data	• 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
Control Domains Covered	• Security • Availability • Confidentiality • Processing Integrity and/or • Privacy	• Transaction processing controls • Supporting IT general controls
Level of Standardization	• Principles selected by service provider. • Pre-defined criteria used rather than control objectives.	• Control objectives defined by service provider and may vary depending on the type of service provided.

Applicability of Trust Services Principles

Domain	Trust Services Principle	Trends Regarding 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, non-financial 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 SOC1 reports

Applicability of Trust Services Principles (continued)

Domain	Trust Services Principle	Trends Regarding Applicability
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. • Applicable where a service provider is entrusted to maintain the confidentiality of an enterprise customer's data of all types.
Processing Integrity	• System processing is complete, accurate, timely, and authorized.	• Potentially applicable for a wide variety of non-financial 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 and regulatory frameworks.	• 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.

SOC2/SOC3 Criteria Summary

Security		
■ Security policies ■ Security awareness and communication ■ Risk assessment ■ Threat identification ■ Information classification	■ Logical access ■ Physical access ■ Security monitoring ■ Incident management ■ Encryption	■ Personnel ■ Systems development and maintenance ■ Configuration management ■ Change management ■ Monitoring / compliance

Availability	Confidentiality	Processing Integrity	Privacy
■ Availability policy ■ Backup and restoration ■ Environmental controls ■ Disaster recovery	■ Confidentiality policy ■ Confidentiality of inputs, data processing, and outputs ■ Information disclosures ■ Confidentiality of Information in systems development	■ System processing integrity policies ■ Completeness, accuracy, timeliness, and authorization of inputs, system processing, and outputs ■ Information tracing from source to disposition	■ Management ■ Notice ■ Choice and consent ■ Collection ■ Use and retention ■ Access ■ Disclosure to third parties ■ Quality ■ Monitoring and enforcement

Contrasting the level of detail provided by SOC 2 and SOC 3 reports

	SOC 2	SOC 3
Common benefits	▪ Detailed examination based on defined Criteria for Security, Availability, Confidentiality, Processing Integrity, and/ or Privacy ▪ Report includes a brief system description ▪ Report includes management's assertion regarding controls	▪ Where subservice providers are used, management may include its monitoring controls over of those operations.
Unique benefits	▪ SOC 2 is more flexible than SOC 3 for the service provider in that it permits carve out of supporting services provided by subservice providers. ▪ SOC 2 includes detail on the service provider's controls as well as the auditor's detailed test procedures, and test results, enabling the reader of the report to assess the service provider at a more granular level.	▪ SOC 3 provides an overall conclusion on whether the service provider achieved the stated Trust Services Criteria, and the user does not need to digest pages of detailed control descriptions, and test procedures. ▪ If the service provider meets all of the Criteria, it may choose to display the SOC 3 seal on its Web site which links to the SOC 3 report.
Potential drawbacks	▪ The user may need to obtain additional reports from significant subservice providers to gain comfort over their activities. ▪ The user may not want to review the detail of the report (controls, tests, etc.) rather than an overall conclusion. ▪ Service providers may not be willing to share a detailed report due to concerns regarding disclosing sensitive information (i.e., detailed security controls).	▪ SOC 3 does not permit carve-out of significant subservice provider activities. If it is not feasible to cover those activities as part of the service provider's audit, SOC 3 is not an available option. ▪ If one or more of the Criteria are not met, the service provider would not be able to display the SOC 3 seal until the issue(s) are corrected, and re-audited.

SOC report structure

Traditional SAS 70	SOC1	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*

Effectively Using SOC Reports

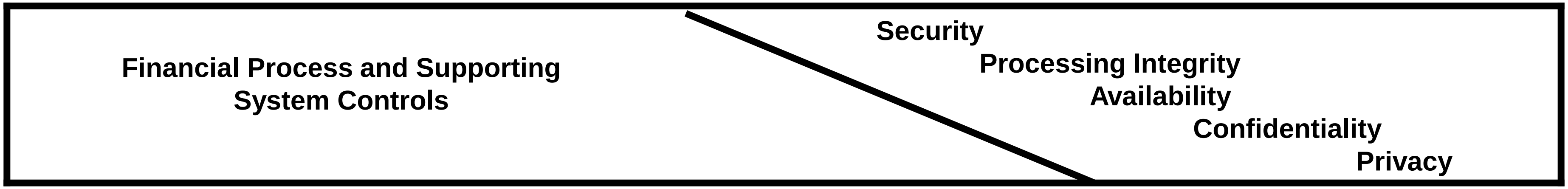
SOC Reports for Different Scenarios

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

- Financial services
- Asset management and custody 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
- Any service where customers' primary concern is security, availability or privacy



Financial Process and Supporting System Controls

Security
Processing Integrity
Availability
Confidentiality
Privacy

Using SOC Reports to Streamline Vendor Questionnaire Processing and Assist with Regulatory Compliance

- The SOC2 report can serve as a tool to:
  - Answer questions that would ordinarily be included in vendor questionnaires
  - Assist user organizations in addressing regulatory compliance requirements such as those imposed by SOX-404 and Data Protection law and other local regulatory requirements (i.e.BoG Governors's act 2577/2006)
- As shown below, the service provider could include a mapping table in the Other Information section of the SOC2 report showing how their controls align with common vendor security questionnaire topics or the requirements of a specific standard/regulation (for example, ISO 27001/27002).

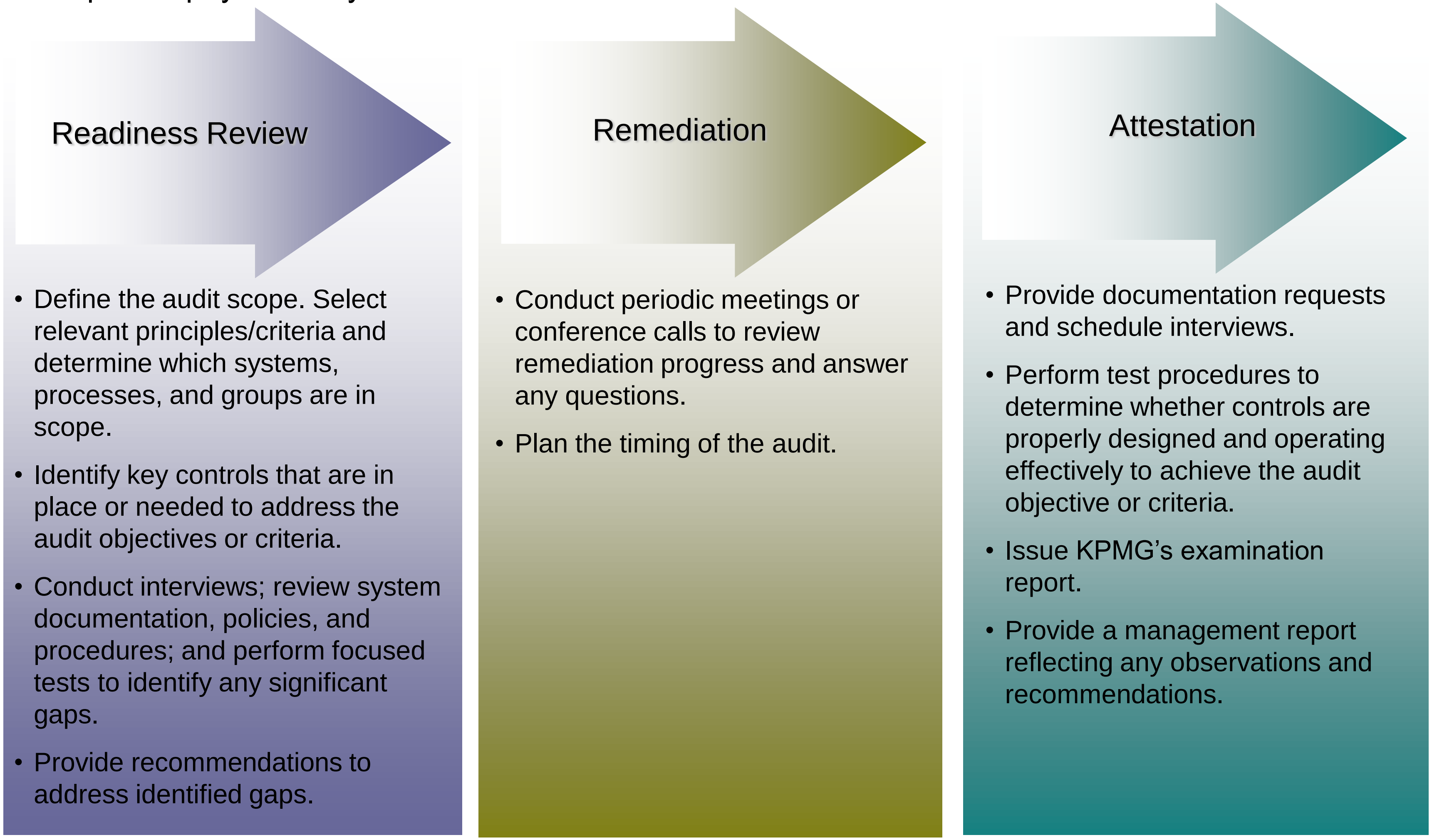
SAMPLE – Relation of Service Provider's Controls to ISO 27001/27002 Control Objectives

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	Related Service Provider Controls
A.5.1 Information security policy	1.01.01, 1.02.01
A.6.1 Internal organization	1.03.01
A.6.2 External parties	1.02.02
…	…

Our IT Attestation Methodology

The following diagram provides an overview of our IT Attestation approach. It reflects our “Manage to Success” philosophy for first year audits.



Readiness Review

- Define the audit scope. Select relevant principles/criteria and determine which systems, processes, and groups are in scope.
- Identify key controls that are in place or needed to address the audit objectives or criteria.
- Conduct interviews; review system documentation, policies, and procedures; and perform focused tests to identify any significant gaps.
- Provide recommendations to address identified gaps.

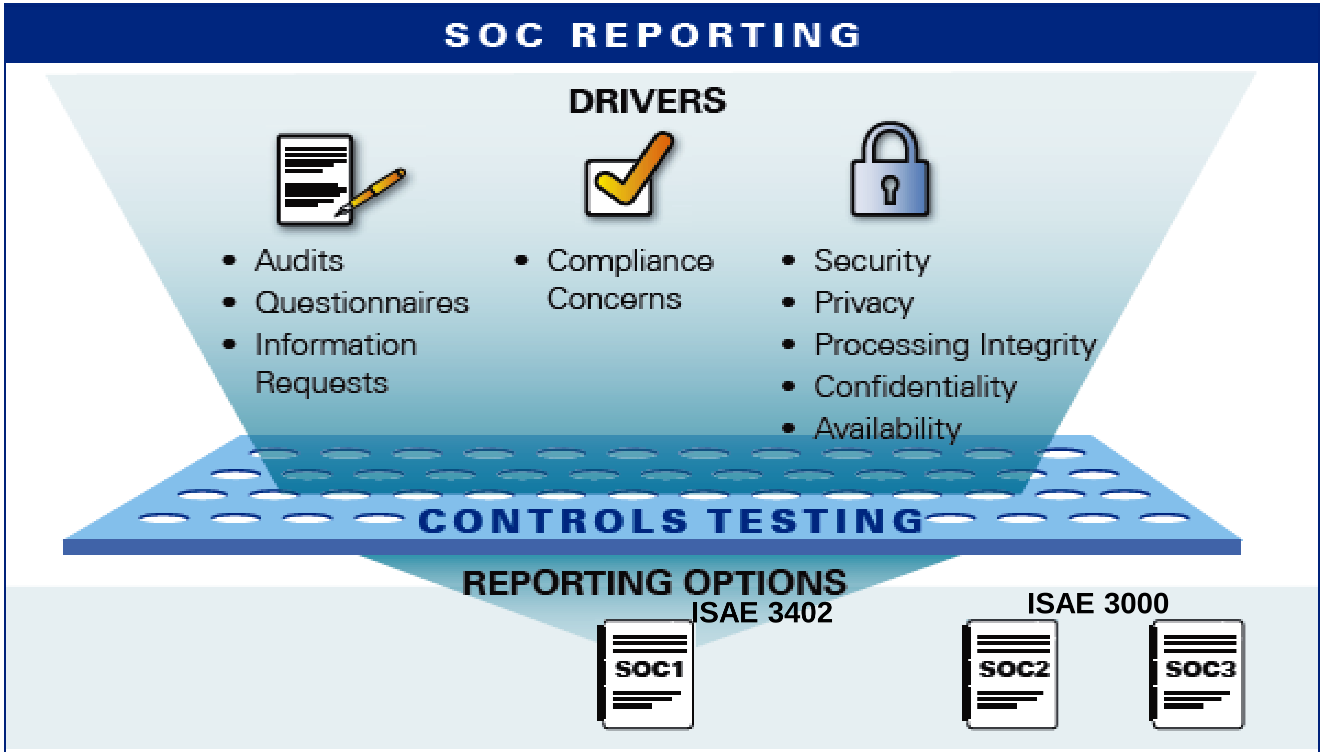
Remediation

- Conduct periodic meetings or conference calls to review remediation progress and answer any questions.
- Plan the timing of the audit.

Attestation

- Provide documentation requests and schedule interviews.
- Perform test procedures to determine whether controls are properly designed and operating effectively to achieve the audit objective or criteria.
- Issue KPMG’s examination report.
- Provide a management report reflecting any observations and recommendations.

Conclusion



SOC REPORTING

DRIVERS

- Audits
- Questionnaires
- Information Requests

- Compliance Concerns

- Security
- Privacy
- Processing Integrity
- Confidentiality
- Availability

CONTROLS TESTING

REPORTING OPTIONS

ISAE 3402

ISAE 3000

BENEFITS	
Service Organization	- Provide a competitive advantage - The SO can avoid unexpected audits - Assist in building trust & confidence - SOC2/3 can incorporate other publically available frameworks such as ISO 2700x, PCI/ etc.
User Organization	- Provide an independent assessment - Assist with regulatory compliance - Reduce the possibility of additional audit costs - Increase audit efficiency

Q & A

KPMG

cutting through complexity™

Thank You