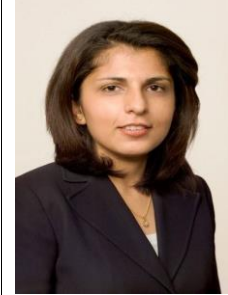


**Enhancing Vendor Risk & Compliance
Management Using SOC2 & SOC3 Reports**

Mark Lundin
Partner, KPMG LLP
Reema Anand
Director, KPMG LLP



Professional Techniques – T22

Session Abstract

Customers of outsourced service providers are increasingly challenged to ensure that their service providers have sufficient safeguards in place to protect sensitive business and customer data, ensure the availability of key systems and services, conduct system processing completely and accurately, and help achieve applicable regulatory or other compliance requirements.

Service organizations are also burdened with a growing number of customer requirements for the completion of detailed questionnaires, varying types of onsite customer audits, different types of audit reports, and evidence of compliance with differing standards and regulations.

Service Organization Control (SOC) reports, particularly SOC2 and SOC3, can be a highly effective tool for understanding the controls in place at a service organization and gaining independent assurance over their design and effectiveness to help manage risk and compliance obligations.

This session will provide:

- User guidance for effectively leveraging SOC2/SOC3 reports as part of a vendor risk and compliance management program
- Service organization guidance for planning and scoping SOC2/SOC3 examinations and customer communication programs to help reduce the burden of customers' risk management and compliance activities
- Examples of enhanced SOC2 reporting to demonstrate alignment with additional standards or frameworks where helpful to address common customer requirements
- Specific discussion of the use of SOC2/SOC3 for cloud service providers

Target Audience

Business and IT professionals with responsibility for vendor risk management, IT governance, IT compliance, or maintaining compliance with IT-focused customer and regulatory requirements.

COBIT Objectives or Processes

Provides Processes for Governance of Enterprise IT to Monitor/Evaluate/Assess, and Manage Suppliers, Manage Risk, Manage Security,

Speaker Bio

Mark Lundin

Mark is a Partner in KPMG's Risk Consulting practice based in San Francisco focused on the technology sector and Cloud/Internet services. He serves a variety of market leading and emerging technology companies and heads a team focused on cloud, security and privacy audit and consulting. Mark has participated actively in ISO and other standards organizations focused on these topics for over 10 years.

Reema Anand

Reema is a Director in KPMG's Risk Consulting practice based in Santa Clara with more than 9 years of information technology advisory and business experience. She focuses on providing cloud and security assurance services to address operational, technology and security risks for a variety of technology service providers. She also has a strong background in consulting services related to public key infrastructures (PKI) and the use of cryptography and encryption technologies and actively participates in the development of related industry security standards.

Speaker Details (optional):

Company	KPMG
Title	Mark Lundin, Partner
Facebook URL	
Twitter URL	
LinkedIn URL	www.linkedin.com/in/lundinmark/
E-mail	mlundin@kpmg.com
Website	www.kpmg.com

Speaker Details (optional):

Company	KPMG
Title	Reema Anand, Director
Facebook URL	
Twitter URL	
LinkedIn URL	http://www.linkedin.com/pub/reema-anand/5/132/906
E-mail	reemaanand@kpmg.com
Website	www.kpmg.com