

**Audits of Controls at a Service Organization: New
Standards SSAE 16 and ISAE 3402**

Sumit Kalra and Duff Donnelly, Grant Thornton LLP



Governance, Risk & Compliance Track – Session G24

Abstract:

Whether you are a provider, buyer or just considering the use of third-party services, you will likely be impacted by the changing standards related to various compliance programs. Whether your focus is on industry-specific requirements or other relevant topics such as information security, this session will provide information by which you can develop an action plan to address upcoming changes to the SAS 70 standard.

Key objectives addressed in the presentation:

- Background on the new standards
- Key differences between SAS 70 and SSAE 16
- Key differences between SSAE 16 and ISAE 3402
- 10 steps for transition success
- Considerations before adopting

Applicability:

- Educate their organizations regarding the key differences between SAS 70 and the SSAE 16
- Develop a roadmap to transition to the new standard

Target Audience:

- Skill level: Intermediate and advanced
- Occupation: Audit, consumer of third-party services, security, compliance, finance, sales account managers, layperson, IT operations, etc.
- Occupational Experience: Entry-level, senior, manager, director, VP, partner, CISO, CFO

COBIT Objectives:

PO5 Manage the IT Investment
PO8 Manage Quality
PO9 Assess and Manage IT Risks

AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI5 Procure IT Resources

DS1 Define and Manage Service Levels
DS2 Manage Third-party Services

ME2 Monitor and Evaluate Internal Control
ME3 Ensure Regulatory Compliance



Speaker Bio:

Duff Donnelly is a Senior Manager in the Greater Bay Area Business Advisory Services (BAS) practice. Duff has over 20 years of industry and consulting experience, focused on business and IT risk management, internal audit, technology quality assurance, technology effectiveness, system selection and implementation, litigation support, merger integration, and project management for the biotech, healthcare, technology and manufacturing industries.

Sumit Kalra is a Senior Manager in the Greater bay Area Business Advisory Services (BAS) practice. Sumit has over 10 years of experience providing information technology management and risk management at several firms in various industries (Financial services, consumer retail and technology). While he leads the SAS70 and IT audit services for San Francisco/ Bay Area practice, he has significant experience in information systems auditing, review of legislations / standards (i.e. COBIT, ISO 17799 / 24001, GLBA, FFIEC, PCI AND TG3) impacting IT Operations and information security management.