San Francisco – 2010 ISACA Fall Conference
Speaker Information

GRC (Pro)(Con)Fusion – Tools, Processes, and Pitfalls

Jason Kobus, SVB Financial Group

Core Competencies Track – Session C32

Abstract:

This presentation will be a vendor-agnostic presentation of key aspects of Governance Risk and Compliance (GRC) tool and process interaction to help practitioners within their own environments. One problem facing many practitioners today is that the GRC space is saturated with a multitude of products offering some degree of enterprise, IT or niche GRC capability. The presentation will discuss how to narrow down the requirements, engage stakeholders, and provide strategies to select, and obtain funding for, GRC tools.

However, a tool does not automatically equate to compliance, so the presentation will explore critical success factors required to align people, processes and technology in the GRC space. Concepts which will be covered include how to "test once and comply with many requirements", and how to improve communications using a "risk management backplane", to reduce duplication of assessment efforts and target areas of common risk.

Attendees will leave with a tool set of criteria they can use to make more informed decisions about GRC issues such as tool selection criteria, how to integrate tools into processes, and how to avoid common pitfalls.

Target Audience:

The presentation will be directed at intermediate level practitioners with experience in one or more of the following fields: audit, information security, IT risk, enterprise risk, data privacy, business continuity, and compliance. It will also be helpful for managers who either make or influence decisions about resource allocation or budget in GRC projects, processes, and technologies.

COBIT Objectives:

ME2 Monitor and Evaluate Internal Control
ME3 Ensure Compliance With External Requirements
ME4 Provide IT Governance
PO4.8 Responsibility for Risk, Security and Compliance
PO9.1 IT Risk Management Framework
AI1 Identify Automated Solutions
DS5.1 Management of IT Security

Speaker Bio:

In addition to several rounds of GRC product evaluation and first hand user experience, Jason has hands-on IT experience with building in-house GRC databases and reporting tools. He currently manages GLBA, Privacy and FACTA Red Flags programs at SVB Financial Group. He has held prior roles as VP/Information Security & Privacy Officer with Merrill Lynch and auditing and consulting with Deloitte's Enterprise Risk Services. He was co-chair of the SF-ISACA Education Committee and CISM workshop instructor between 2005-2007. He holds CISA, CISM, CISSP, CIA, CIPP, and PMP credentials.