Using Risk Portfolio Management and Self-Assessments to Mitigate Risk

Michael Zanaglio and Rajiv Agarwal, Wells Fargo

Professional Techniques Track – Session T23

Abstract:

Whether bottom up or top down, the aggregation, prioritization and tracking of real risk is increasingly critical for an organization. The risk portfolio management process provides the operational risk manager to examine operational risk at the business unit, line of business and enterprise perspective. The foundation of a successful risk management mitigation strategy begins with a Risk Portfolio Management (RPM) program. This presentation will show how to build a Risk Portfolio Management program utilizing a risk framework. Once the framework is selected and the strategy developed, the mapping of all risks to policy, standards and requirements is required to conduct the self assessment program.

This presentation will further show how to review the self assessment program. The review of the risk framework, self assessment process and empirical results will ensure effective risk mitigation.

While process driven, the review will demonstrate how to recognize and mitigate risks using a documented, repeatable process that includes continuous monitoring and review. The review and monitoring will provide management with real risk mitigation and allow the review team the ability to indentify: exceptions, outliers and occurrences that may indicate risk that surpasses risk tolerance and thresholds.

Target Audience:

The target audience for this presentation consists of risk management professionals.

Skill level: Intermediate / Advanced
Occupation: Audit, Security, Operational Risk Managers
Occupational Experience: Senior, Manager, Director

COBIT Objectives:

The risk management activities covered in this presentation rely on COBIT as the risk management framework for the organization and address all the control objectives as an over-arching umbrella. The activity of Technology Self Assessment and Risk portfolio Management address the following specific COBIT Control Objectives:

- PO4 Define the IT processes, organization and relationships
- PO6 Communicate management aims and direction
- PO9 Assess and manage IT risks
- DS4 Ensure continuous service
- ME2 Monitor and evaluate internal control
- ME3 Ensure compliance with external requirements
- ME4 Provide IT governance

Speaker Bio:

Michael Zanaglio began his career at Mellon Bank in consumer loan auditing. Most recently he has led a team in Wachovia Investment Bank of operational risk management and today is the operational risk manager for the Wells Fargo Wholesale technology Services Organization. He and his team serve as Single Point of Contact (SPOC) for audit, government and external agencies as well for the past five years. His team has maintained a zero significant deficiency SOX score, eliminated key issues and reduced “red” or non-compliant items to risk tolerance acceptable levels. They initiated the RPM and self assessment process five years ago after inventorying the entire portfolio of risk and establishing a Single Point of Contact (SPOC) relationship with all individuals and agencies for consistent, effective and efficient risk mitigation.

Rajiv Agarwal is an Operational Risk Manager for Wholesale Technology Services organization at Wells Fargo. He and his team manage the oversight and governance activities for some key areas including Risk Portfolio Management. Rajiv is a certified Six-Sigma Black Belt and is currently working on ISACA’s CGEIT certification.