

**Conducting Enterprise-wide IT Risk Assessments**

Lance M. Turcato, City of Phoenix - City Auditor Department



Professional Strategies Track – Session S11

**Abstract:**

Essential to IT governance and IT audit planning is a comprehensive process for managing IT risks. A risk management framework helps ensure integration of business, operational, and IT risk management, risk assessment, and risk mitigation strategies. Furthermore, formal risk management establishes a common and agreed-upon level of IT risks, mitigation strategies, and accepted residual risks. A key component of risk management is a comprehensive risk assessment process. On a recurring basis, IT risks should be re-evaluated to assess the likelihood and impact of all identified risks using qualitative and quantitative methods. Furthermore, the probability and impact associated with inherent and residual risk should be determined individually, by category, and on a portfolio basis. This session will discuss a methodology for completing an enterprise-wide IT risk assessment in highly decentralized and diverse environments. Session attendees will be provided with access to templates and references to resources that can be used immediately to conduct enterprise-wide risk assessments in their organizations.

**Target Audience:**

Skill level – intermediate  
Occupation – auditors, security, risk management, compliance  
Occupational Experience – senior and above

**COBIT Objectives:**

COBIT PO9 and the RiskIT Framework

**Speaker Bio:**

**Lance Turcato** is Deputy City Auditor at the City of Phoenix. Lance manages the IT Audit Division and leads IT compliance efforts at the City. Prior to working at the City, Lance was Managing Director of Technology Infrastructure & Security Oversight at Charles Schwab & Co., Inc. Prior to joining Schwab, Lance was a senior IT security consultant with Price Waterhouse LLP and Coopers & Lybrand LLP prior to the merger of those firms.

Lance is a CGEIT, CISA, CISM, CPA, and CITP and holds a Bachelor degree (Accounting) and a Masters degree (Accountancy & Information Systems). He has extensive experience managing and conducting reviews of complex technology infrastructures for businesses in a wide variety of industries. Lance has taught accounting and information technology courses at major universities and is a regular speaker at local, regional, and international technology governance, control, and security conferences.

Lance currently serves the Phoenix ISACA Chapter as Vice President and also Chair of the Communications Committee. Lance actively served on the San Francisco ISACA Chapter Board for a number of years in various capacities including President, Vice President, CISA Coordination Committee Chair, and Communication Committee Chair. Lance received the "President of the Millennium" Award in 1999. Lance is also actively involved in ISACA International initiatives including SME reviews of updates to COBIT materials.