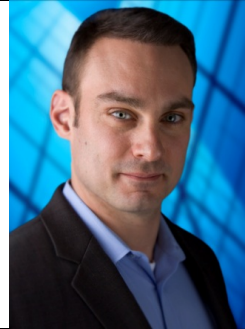## The Future of the Advanced Security Operations Center (SOC)

Philip Aldrich

Program Director, Risk Management – EMC & RSA

Governance Risk and Compliance – G11

Session Abstract

The Future of the Advanced SOC: Developing a platform for more effective security management and compliance

In today's world of advanced threats and complex compliance issues it's no longer feasible for an organization to resist every attack or manage security based on compliance pressures. There are no more castle walls to keep back the horde. A more realistic goal is for security operations teams to be fluid, reacting quickly to determine how an attack happened, reduce the 'attacker free time', and put measures in place to prevent similar future attacks. All while automating the proof of compliance process.

In this presentation, we will discuss how organizations can manage risk more efficiently and secure trust in IT through comprehensive visibility, actionable intelligence, and advanced security analytics for fast detection and investigation.

Target Audience

Anyone interested in gaining a better understanding of Security Management, Security Analytics and the notion of the Advanced Security Operations Center

COBIT Objectives

EDM03: Ensure Risk Optimization
APO12: Manage Risk
APO13: Manage Security
DSS02: Manage Service Requests and Incidents
DSS04: Manage Continuity
DSS05: Manage Security Services

Speaker Bio

Currently, Phil Aldrich is responsible for the enterprise Governance, Risk and Compliance (GRC) program development and implementation at EMC. He reports directly into EMC's Chief Risk Officer (CRO) and coordinates GRC activities with a variety of internal teams such as internal audit, information security, product security, CIRC and operational risk management. Previously, Phil was responsible for the product strategy and development for the RSA Archer EGRC Suite at RSA. Prior to joining EMC/RSA he managed Information Security globally for a Fortune 500 company and implemented an enterprise GRC program. Phil graduated from the United States Military Academy at West Point, commissioned as a helicopter aviation officer and served most of his time overseas. He holds 2 master degrees from Boston University in security and technology innovation, as well as, CISSP, CISM, CRISC, CIPP and CISA certifications.