Enabling Technology to Automate GRC

Monica McDermott, Agiliance – IT GRC
Jennifer Ellard, Symantec - DLP
TBD, EMC – eDiscovery
Sid Sinha, Oracle – Financial GRC
Narayan Makaram, ArcSight - SIEM

PHOTO

In-Depth Seminars Track – Session D3

Abstract:

With the myriad of GRC technologies to choose from, organizations have a difficult time determining what will best solve their security, risk and compliance requirements. Learn how top leading vendors help to automate facets of GRC. Technology as defined by Gartner that will be reviewed:

1. IT GRC – IT governance, risk and compliance management technology supports the management, measurement and reporting of IT controls; the distribution and attestation of policies; compliance reporting; and risk assessment. IT GRC solutions have policy and asset repositories, basic document management, workflow, survey and reporting functionality, and dashboarding. IT GRC solutions provide policy content that is specific to IT controls, as well as support for automated measurement and reporting. The products may take input from control automation and monitoring tools, such as vulnerability assessment, configuration auditing, identity and access management, security information, and event monitoring.
2. Financial GRC - Financial GRC offerings target to the needs of the CFO and finance function. It combines elements of ERP, financial governance, risk and compliance management, and Corporate Performance Management
3. DLP – Data loss prevention tools enable the dynamic application of policy based on the classification of content determined at the time of an operation. They are used to address the risk of inadvertent or accidental leaks or exposure of sensitive enterprise information outside authorized channels using monitoring, filtering, blocking and remediation features. DLP technologies include hardware and software solutions that are deployed at the endpoint (desktop and servers), at the network boundary and within the enterprise for data discovery purposes, and they perform deep content inspection using sophisticated detection techniques that extend beyond simple keyword matching (for example, advanced regular expressions, partial document matching, Bayesian analysis and machine learning). DLP products maintain detailed logs that can be used to support investigations.
4. SIEM – Security information and event management (SIEM) technology provides two main capabilities. Security information management (SIM) provides log management — the collection, reporting and analysis of log data — to support regulatory compliance reporting, internal threat management and resource access monitoring. Security event management (SEM) processes log event data from security devices, network devices, systems and applications in real time, to provide security monitoring, event correlation and incident response.
5. E-discovery- Electronic discovery software facilitates the identification, collection, preservation, processing, review, analysis and production of large amounts of electronically stored information (ESI) within an enterprise to meet the mandates imposed by common-law requirements for discovery. These demands may be due to civil or criminal litigation, regulatory oversight or administrative proceedings.

Target Audience:
VPs, CIOs, Sr. Managers, IT System Designers, Security Professionals, IT Auditors.
COBIT Objectives:
GRC and/or IT GRC informational managers map COBIT control objectives to controls. In this way, organizations are monitoring all COBIT objectives along with multiple standards and regulations. This is known in the industry as a common control framework (CCF).
Speaker Bio: