



## Dan Highman

### Security Metrics, Reporting to the Board

Ever tried to find good information security, information protection, information risk management, operational security risk management or cyber security metrics for reporting to boards? It's difficult. As part of Critical Infrastructure Protection, NERC has commissioned a committee to define cyber security metrics for energy utilities in the near future, for example. Is the CISO reporting metrics to the board, but the CIO isn't? Is there an Enterprise Risk Management function in the organization? How is operational and corporate risk reported and is it aligned with IT Risk and Information Security? Heat Maps, Risk Trends, report by domain, threats, vulnerabilities and impact? How should you present and what should you present? Join Dan Highman as he explores defining a metrics program, to what level metrics should be reported, industry trends, and what Boards care about. Dan will define metrics and domains and explore different formats of reporting. Interested? Should you be?

### Biography

Daniel P. Highman is the IT Risk Management & Security Practice leader for OpenSky leveraging his 14 years of experience in the areas of Integrated Operational Risk Management, High Availability E-Business Service Oriented Architectures, Information Security Regulatory Compliance, Identity Management, IT Effectiveness, Information Security & Network Architecture, IT Risk Management, and Business Risk Services. This includes creating IT GRC Roadmaps and roadmap implementation services for Fortune 100 clients.

Prior to joining OpenSky, Dan was a manager in Ernst & Young's Technology & Security Risk Services Practice responsible for solution delivery of IT Effectiveness services including IT architecture assessments and alignment to business strategy, program/project advisory, and cost optimization services. Dan advised financial service clients on architecting IT risk management frameworks and FFIEC and GLBA compliance including IT risk assessments. Dan consulted on business risk services to clients including business continuity, integrated risk management, data classification/record retention, and business control process improvements.



## Dan Highman

At Citigroup Insurance Investments, Dan was an AVP responsible for the Information Security, Continuity of Business (CoB), Risk Assessment & Management, Facilities Services, and Vendor Management programs. Prior to Citigroup, Dan was a Senior Network Systems Consultant with International Network Services where he consulted on IT portfolio rationalization and business alignment, IT program management, and IT expense/investment analysis for financial service clients.

Dan is a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), and obtained his Masters of Science degree in Management of Technology from Fairfield University.