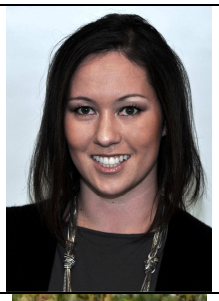
ISACA
Trust in, and value from, information systems
San Francisco Chapter

2011 SF ISACA Fall Conference
Speaker Information

Implementation to Business Value: an ISO 27001 Journey at McKesson

Governance, Risk, & Compliance – G12

Jennifer Burton - IT Risk Management Analyst, McKesson	
Priya Vunnam - IT Risk Management Analyst, McKesson	
Robin Byon - IT Risk Management Analyst, McKesson	
Pierre Fourie - Advisory Services Manager, Ernst & Young	

Session Abstract

This session will provide an overview of the process to create and define a formal Information Security Management System (ISMS), as specified in the ISO/IEC 27001:2005 standard. The speakers will help participants understand how to build a business case to support an ISO 27001 certification effort, as well as how to implement and manage the ISMS. The discussion will cover ISMS methodology, tools, as well as tips on how to integrate ISMS activities into business and security

objectives in the organization.

Target Audience

- IT Security Officers
- IT Managers
- Management Systems Managers
- Professionals involved in introducing ISO/IEC 27001:2005 and ISO/IEC 27002:2005 into an organization
- Chief Security Officers
- Information Security Consultants

Prior review of ISO/IEC 27001:2005, ISO/IEC 27002:2005 and knowledge of information security practices is recommended, but not required.

COBIT Objectives

[*If your session ties to one or more COBIT objectives, please list those here.*]

Speaker Bio

Michelle Nix, MHA, CGEIT, CHPS, GSLC, CRISC

Michelle Nix is a Director of IT Risk Management at McKesson Corporation, a 177 year old Fortune 20 company where she manages the IT Risk Management program for the US Pharmaceuticals division. This division of McKesson generated more than $100B in revenue last year. In this role Michelle interacts with senior management and other risk management groups (internal audit, etc) to provide program level reporting, governance, guidance, education and awareness.

Michelle's background is in health care where she has more than 22 years experience. She has held a number of positions in this industry including pharmaceutical research and development, administration, quality improvement, project management, operations, IT systems support and IT Risk Management. Michelle also has government standards setting experience. Specifically, in California, Michelle is the Co-chair of the California Privacy and Security Advisory Board (CalPSAB) Privacy Committee which focuses on providing state-level privacy standards for health information exchange.

Michelle obtained her Bachelor of Science degree in Biopsychology, Bachelor of Arts degree in Biology from University of California, Santa Barbara and is Masters prepared in Healthcare Administration from Golden Gate University. Her areas of specialty are clinical outcomes, quality improvement, privacy and security for Health Information Exchange models, IT Risk Management and most recently, ISO 27001 standards implementation.

Jennifer Burton, MS, CISA, CISSP, CRISC

Jennifer Burton has held a number of roles at McKesson Corporation, a Fortune 20 company, most recently in the IT Risk Management group. There, she manages IT compliance for the US Pharmaceuticals business unit and provides executive reporting, governance and awareness promotion within the organization.

Jennifer has over 9 years of experience in IT risk management, process improvement, audit, compliance, and security. She earned her Master and Bachelor degrees in Computer Science from the University of California, Davis, where she taught fundamentals and current topics in computer

security. She has consulted at a number of bay area companies and is active in her local San Francisco chapter of ISACA.

Priya Vunnam is an IT Risk and Compliance professional with about 5 years of experience in the field of IT security and compliance. She is currently an IT Risk Analyst at McKesson Corporation, a Fortune 20 company in the health care industry. In her role, she supports the IT Risk Management (ITRM) senior management team in running an enterprise-wide IT Risk Management and Compliance program. She builds processes and tools to support the monitoring of IT compliance for several regulations and standards such as ISO 27001, PCI, HIPAA, SOX, etc. She works with security leaders across several Business Units to perform audits, certification programs such as ISO27001 and SAS70, IT governance, and other related activities. She is the subject-matter expert on Archer (GRC tool), that houses the company's information security policy, security controls, audit results, etc. She also played an instrumental role in the ISO 27001 standards implementation across several Business Units at McKesson.
Prior to joining McKesson, Priya worked for Deloitte as a Security and Privacy consultant. In her consulting career, she worked with several clients helping with PCI compliance, SOX compliance, IT Risk and Security Assessments, Information Security Policy definition and maintenance, and monitoring security controls. She has a Bachelor of Science degree in Computer Science from Jawaharlal Nehru Technological University, India and a Master of Science degree in Information Management from Syracuse University, New York. She is also a certified ISO 27001 Lead Auditor.

Robin Byon is a member of the IT Risk Management group at McKesson and has led a number of ISO 27001 readiness assessments for their various businesses. Robin's background consists of 7 years of public accounting experience at Ernst & Young, which includes assisting clients with identifying and reducing their overall business risk exposure, streamlining IT, business operational controls, and improving process effectiveness (includes IT, business and audit processes). Over the past 3 years, Robin has primarily focused on the information security space, which included areas such as the ISO 27001 framework and the HIPAA/HITECH regulatory requirement.

Pierre Fourie is a Manager in Ernst & Young's Advisory Services practice and has been serving various healthcare and technology clients for over 5 years. Pierre is a CPA with a broad range of experience that includes assisting companies with the development and implementation of Information Security Management Systems and readiness efforts for the ISO 27001 certification process. Pierre has extensive knowledge in the ISO 27001 framework and has lead and facilitated numerous ISO 27001 certification audits. In addition to the information security space, Pierre is heavily integrated with the SAS 70/SSAE 16 standard as well as the SOC reporting framework.