



Session #S33

Presenters:	Bill Robinson, CISSP, Thomas Chimento, Ph.D. CISSP, CISA
Presentation Title:	Leveraging FISMA Guidance to Support an Effective Risk Management Strategy To Secure IT Systems and Meet Regulatory Requirements.
Abstract:	
<p>FISMA is a framework mandated by the Federal Government that uses a Risk Management strategy for 1) categorizing IT systems based upon the information they store, transmit or process; and 2) selecting and implementing appropriate security controls to establish and ensure continuous and sustainable information security. A system security plan that documents the policies, procedures, implementation and continuous monitoring is developed for each information system and must be certified and accredited. Congress tasked NIST (National Institute of Standards and Technology) with the responsibility of developing security standards and guidelines for the federal government, which have broad applicability for both government and corporate security programs and auditing.</p> <p>The first half of this presentation will give an overview of the NIST guidance documents and the certification and accreditation process. The second half will present a series of case studies, providing a lessons-learned approach on how Federal agencies achieve enterprise-wide C&A that simplify, accelerate and report accurate documentation for C&A compliance through FISMA. This presentation demonstrates how agencies such as The Department of Homeland Security, NASA and the US Pacific Air Forces, are dealing with the successes and challenges of a successful Certification and Accreditation Program.</p>	
Target Audience:	
<p>Skill Level: beginner to intermediate Occupation: Auditors, IT Security, anyone who shares any type of information with the Federal Government (vendors, resellers, universities, etc.) Occupational Experience: Anyone with responsibility for auditing, regulatory compliance, or information security.</p>	
COBIT Objectives:	
Speaker Bio:	
<p>Mr. Bill Robinson has more than 15 years of Information Assurance experience for both Federal Government and DoD organizations. As a Senior Information Security Consultant and IA Program Manager for SecureInfo Corporation, Mr. Robinson is responsible for planning and directing quality assurance policies, programs, and initiatives for teams of Information Assurance (IA) Consultants. Mr. Robinson provides senior consultant experience on the DITSCAP/DIACAP, DoDIIS, NISPOM, and NIST SP 800-37 Certification and Accreditation Processes. Prior to SecureInfo, Mr. Robinson served as the Air Force Certification & Accreditation Manager for the Air Intelligence Agency. Mr. Robinson has performed formal Information Systems Certification and Accreditation inspections for DHS, NASA, US Treasury, Library of Congress, US Air Force, US Army, and for Joint Intelligence organizations on behalf of the National Security Agency (NSA) and the Defense Intelligence Agency (DIA). Mr. Robinson is a retired US Air Force veteran who served as a Master Instructor for the Air Education and Training Command.</p> <p>Dr. Thomas Chimento has spent over 10 years as a contractor at NASA in information technology and information security. Starting as a system administrator Dr. Chimento moved quickly into a variety of IT and IS projects. He has evaluated and implemented security solutions for the Ames Research Center and the Agency. For the last two years his focus has been on Agency policies and procedures, regulatory compliance, and FISMA Certification and Accreditation. He is the central liaison between the 10 NASA centers and SecureInfo Corp and provides FISMA guidance and consultation to System Owners and Certification and Accreditation Officials.</p>	