

Session #C11

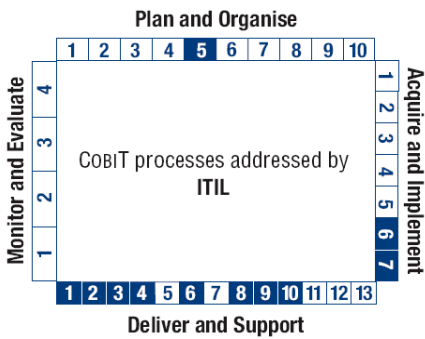
Presenter:	Steve Shofner
Presentation Title:	Introduction To IT Auditing For The Non-IT Auditor
Abstract:	
<p>This is an introductory-level course designed to provide a high-level overview of IT Auditing to non-IT Auditors. It will:</p> <ul style="list-style-type: none"> • Define and discuss objectives, risks, and controls and focus on how similar/dissimilar they are between financial/operational audits & IT audits • Introduce the COBIT framework at a high-level • Discuss the relationship between automated controls (a.k.a. application controls) and IT general controls • Teach attendees how to test IT general controls in a simple environment • Identify characteristics of audit areas when non-IT auditors may want to bring in more expertise (knowing when to call in the experts) 	
Target Audience:	
<p>Anyone interested in gaining a better understanding of what IT Auditors do, or anyone wanting to know how easy it can be to test general controls. Primarily, this would include:</p> <ul style="list-style-type: none"> • Financial auditors • Business users responsible for 'desktop applications,' thereby responsible for supporting the audit of those applications • Business users (or anyone) that want to understand IT general controls and why they matter 	
COBIT Objectives:	
<p>This course will introduce all COBIT areas, but will focus on the following:</p> <p>PO 1-3, 5-6, 8-10 AI 1-4, 6-7 DS 3-5, 8-13 ME 1-2</p>	
Speaker Bio:	
<p>Steve is the IT Audit Manager at Williams-Sonoma, Inc. He recently joined them after ten years of experience with PricewaterhouseCoopers and Ernst & Young, primarily performing external audits and SAS 70 audits. One of his roles with Ernst & Young was the Pacific Northwest Education Coordinator for their IT Audit group. He also spent a rotation in their National practice as a contributor to their IT audit methodologies. He has extensive experience working on integrated audits, which seek to maximize audit efficiencies by relying on IT controls to the fullest extent.</p>	



Session #C12

Presenter:	Miguel (Mike) O. Villegas, CISA, CISSP
Presentation Title:	COBIT Fundamentals and Uses
Abstract:	
<p>This presentation discusses CobiT as a best practice for IT Governance, SOX and Internal Audit. The session will begin with an overview of CobiT fundamentals, differences between 4.0 and 4.1, and details on critical success factors, control objectives and key goal & performance indicators for CobiT processes. It will focus on how CobiT is used to address CIA (confidentiality, integrity and availability). The presentation will also include future direction of CobiT. We will finalize the session with implementation guidelines and possible uses of CobiT. These will assist the participant in using CobiT as a framework or tool in achieving their control objectives.</p>	
Target Audience:	
<ul style="list-style-type: none">• Skill level (all)• Occupation (audit, security, risk management)• Occupational Experience (all)	
COBIT Objectives:	
All COBIT Objectives will be addresses.	
Speaker Bio:	
<p>Mike is past President and current Fall Conference Co-Chair for the SF-ISACA Chapter. Mike was Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance. Previously, he was responsible for Sarbanes-Oxley 404 systems testing, technology compliance, audit liaison services, and controls effectiveness testing. He has over 25 years of Information Systems security and IT audit experience. Mike was previously a partner at Ernst & Young and Arthur Andersen over their information systems security and audit groups over a span of nine years. He has managed several IT Internal Audit departments for two large California banking institutions. He has focused on IT audits and security of mainframe and enterprise environments providing professional consulting services to Fortune 1000 companies across all industries. Mike is currently involved in several ISACA CobiT research initiatives and was on the project working group for ISACA's Net Centric (Intranet/Extranet/Internet) Control & Security publication. Mike is a Certified Information Systems Auditor (CISA) and a Certified Information Systems Security Professional (CISSP).</p>	

Session #C13

Presenters:	Chad Kalmes & Paulina Fraser
Presentation Title:	Beyond SOX: Adopting ITIL
• Abstract:	
<p>Organizations are increasingly dependent upon IT to satisfy their corporate aims and meet their business needs. This growing dependency has been especially apparent with the introduction of Sarbanes-Oxley, as both business and IT have become accountable for the completeness and accuracy of financial statements. At the same time, IT departments are seen by the rest of the organization as cost centers and are being asked to increasingly cut costs.</p> <p>While ITIL was not conceived with SOX in mind, it does define the consistent, repeatable, auditable and verifiable practices needed to access and track the data vital for compliance. In our presentation, we will discuss how ITIL can help companies become SOX-compliant, while at the same time helping to reduce the costs of managing the IT organization and moving it from a reactive (firefighting) to proactive (managed) mode. We will talk about the benefits of implementing ITIL, address the links between ITIL- and SOX-compliance, and touch upon some potential problems that may be encountered during an ITIL implementation.</p>	
• Target Audience:	
<ul style="list-style-type: none"> • Skill level: Beginner • Occupation: Audit • Occupational Experience: Entry level 	
COBIT Objectives:	
	
Speaker Bio:	



San Francisco – 2007 ISACA Fall Conference Presenter Information

Chad Kalmes is a Senior Manager with Protiviti's Technology Risk practice in the Bay Area. He leads the Bay Area ITIL practice, co-leads the Bay Area security practice, and is a member of Protiviti's national security team. Chad has over 9 years of consulting experience, focusing on the relationship between business processes and technology, and assisting clients in defining and managing the risks associated with their IT environments. He has led numerous IT Strategy, Security & Privacy, ITIL, IT General Controls, and IT Audit engagements across all major industry groups. Aside from helping clients identify and manage their compliance with various state and federal regulations (Sarbanes-Oxley, HIPAA, GLBA, SB1386, PCI, etc.), he has assisted numerous clients with developing the roadmap for managing their IT organizations in a cost-effective and efficient manner. Chad graduated from the University of Notre Dame with a BBA in Management Information Systems (MIS) and focus in International Business. Chad currently holds his CISA and CISSP-ISSMP certifications. He is a member of the IIA, ISACA, ISC2, and the Silicon Valley Leadership Group (Federal Issues Committee).

Paulina Fraser is a Manager with Protiviti's Technology Risk practice in the Bay Area. She leads the Bay Area ITIL practice and is a member of the Application Controls Effectiveness (ACE) team. Paulina has over 5 years of consulting experience in the areas of risk management, technology management, and business process reengineering. She has led numerous ITIL, ACE, and IT General Controls audit engagements across all major industry groups. In addition, she has taught several classes on project management best practices and audit approach. Paulina graduated from Dartmouth College with a BA in Economics and obtained an MBA in Technology Management from the University of California, Davis. She currently holds CISA and PMP certifications and is a member of ISACA, IIA, and PMI.



Session #C21

Presenter:	Tony Goulding
Presentation Title:	Leveraging IT Audit Resources – IT Risk Assessment Trough High-Impact Audits
Abstract:	
<p>Over the last few years, companies (especially the larger) have begun to understand the value of automating their manual controls in response to business needs: manage cost; manage risk; comply with regulations; and aligning IT to the needs of the business. In this presentation, you will learn about one of the more mature and ubiquitous forms of IT security controls – Access Control.</p> <p>This session will focus on user Authentication and Authorization via the more common approaches – Web Access Control, Host-Based Access Control, and Single Sign On. The audience will gain an understanding of the issues being solved, typical approaches used to implement such controls and where the points of audit lie.</p> <p>The session will wrap-up with a brief introduction to some of the more bleeding-edge aspects of Access Control that companies are exploring – Federation and SOA Security – to give the audience a heads-up on future direction.</p>	
Target Audience:	
COBIT Objectives:	
Speaker Bio:	
<p>Mr. Goulding is the Western Regional Principal Consultant for security at CA Inc. In this capacity, he focuses on evangelizing CA's eTrust brand of security solutions and providing technical and business strategy to the regional sales force. Mr. Goulding consults in the areas of Identity, Access, Threat, and Security Information Management with a focus on role-based identity, entitlement management, directory infrastructures, regulatory compliance, authentication methods, and PKI. In addition to his individual contributor roles, Mr. Goulding's career has included a number of senior management positions in product marketing, professional services, pre-sales consulting and customer support. He has served as Practice Director for three Silicon Valley software security companies, managing P&L for Professional Services covering both North America and Europe. In this role, he led many teams responsible for design, development and implementation of enterprise-wide security solutions for Fortune 500 clients nationally and internationally. Mr. Goulding was also co-founder of a Silicon Valley company focused on building services practices and methodologies for companies specializing in security services and security software solutions. Educated in England and Wales, U.K., Mr. Goulding holds a Bachelor of Science degree with Honors in Mathematics. He is a CISSP- and ITIL-certified security professional with over 22 years of industry experience.</p>	

Session #C22

Presenters:	Ray Cheung and Biniam Debrezion
Presentation Title:	Introduction to Change Management
Abstract:	
<p>This is an introductory-level course designed to provide a high-level overview of Change Management. The following are the areas that will be covered</p> <ul style="list-style-type: none"> • Discuss types of changes in production environment • Discuss the Change Management Policies and Procedures and their requirements • Discuss implementing, evaluating and enforcing Change Management controls • Discuss the impact of weak Change Management controls • Discuss methods of detecting unauthorized changes 	
Target Audience:	
<p>This course targets any individual who is interested to understand the basic elements of Change Management. This may include</p> <ul style="list-style-type: none"> • IT Auditors • Production environment managers • Individuals who implement changes to production systems. 	
COBIT Objectives:	
<p>This course will addresses the following COBIT objectives:</p> <ul style="list-style-type: none"> • COBIT objective 2.1 (Internal Control Monitoring) • COBIT objective 2.2 (Major Changes to Existing Systems) • COBIT objective 3.4 (System Software Installation) • COBIT objective 3.6 (System Software Change Controls) • COBIT objective 4.10 (Segregation of Duties) • COBIT objective 5.12 (Promotion to Production) • COBIT objective 6.1 (Change Request Initiation and Control) • COBIT objective 6.3 (Control of Changes) • COBIT objective 6.4 (Emergency Changes) • COBIT objective 6.6 (Compliance with Policies, Procedures and Standards) • COBIT objective 11.6 (System Development Life Cycle Methodology for Major Changes to Existing Technology) • COBIT objective 6.7 (Software Release Policy) 	
Speaker Bio:	

Mr. Cheung is a director in KPMG's Risk Advisory Services (RAS) practice located in San Francisco and has over 18 years of experience solving business problems by identifying control inefficiencies through implementation of technology and process improvements. Mr. Cheung has significant experience in providing independent Board and senior management level consulting services to improve client's technology risk management processes. He has served as acting Chief Information Officer for clients in carrying out all management responsibilities by leading a cross-functional project team. The responsibilities included change management, internal audit program planning, strategy alignment, IT outsourcing management, technology selection and implementation, and enterprise information security and privacy. Prior to joining KPMG, Ray was a Regional Director for BDO Seidman, a Vice President of the Technology Management Group at Visa International, and a Senior Manager with the Risk Consulting practice at Andersen.

Biniam is a senior associate in KPMG's Silicon Valley Advisory Services practice with over 10 years of technical experience using emerging technologies to resolve business problems. Mr. Debrezion is also experienced in evaluating existing system security weaknesses, identifying control gaps, and communicating better implementation control and security plan. His managerial and analytical skills include communication, analytical, and multitasking capabilities.



Session #C24

Presenters:	Matthew Hatch, Oliver Petri
Presentation Title:	Introduction to Application Controls
Abstract:	
<ul style="list-style-type: none">• Application Controls Defined• The value of application controls• Common testing approaches for application controls• Common misconceptions about application controls	
Target Audience:	
<ul style="list-style-type: none">• Skill level – Beginner & Intermediate• Occupation – Audit, Application development/support personnel, Internal Audit / SOX• Occupational Experience – All	
COBIT Objectives:	
<ul style="list-style-type: none">• PO4• PO5• AI7• DS11	
Speaker Bio:	
<p>Matt is a Senior Manager in Ernst & Young's San Francisco office within the Risk Advisory Services Practice (RAS). Matt has over eight years experience leading large international projects including SOX advisory services, Integrated Audits, and ERP program assurance initiatives. Matt has extensive experience serving the life sciences and high tech industries in the bay area. Matt serves as the area ERP Champion within Ernst & Young's Pacific North West team which includes training, quality and business development responsibilities. Matt is a California CPA and holds a CISA certification from ISACA. Matt has a BS degree in Accounting and Management Information Systems from California State University, Chico.</p> <p>Oliver is part of the Risk Advisory Services Group at Ernst & Young where he is responsible for managing the information systems portion of financial audits for major corporations. He is a subject matter resource for data analytics and computer assisted auditing techniques used in external audit projects. He has more than 4 years of experience in identifying and auditing application controls and teaches IT auditing classes for Ernst & Young on a national level. Prior to joining Ernst & Young, he worked in the field of Technology Consulting. Oliver holds a CISA certification from ISACA and served as a board member on the ISACA Silicon Valley chapter. Oliver holds an MBA degree from the Kansas State University and an undergraduate degree in Business and Economics from the University in Giessen, Germany.</p>	

Session #C31

Presenter:	Scott Hayes
Presentation Title:	Intro to Database Auditing
Abstract:	
<p>Database Auditing for Compliance & Security:</p> <p>Compliance with regulatory obligations such as Sarbanes Oxley, HIPAA, PCI and GLBA forces companies to implement segregation of duties and adopt increasingly onerous monitoring and reporting policies. Sensitive information assets and privileged users in particular must be monitored to demonstrate the existence of detective controls while proving the efficacy of preventative controls.</p> <p>Scott Hayes will discuss how "Big 4" audit findings and interpretations of compliance obligations are being translated into specific directives for database auditing. Scott will discuss:</p> <ul style="list-style-type: none"> • What are the most common database auditing, monitoring, and reporting requirements for compliance? • Auditing Privileged Users - the importance of monitoring administrators, developers, and outsourcers • Security vulnerabilities to your data and spotting anomalous behavior • Specific suggestions: Questions for audit to ask and IT to answer <p>In addition to answering these questions and providing stories from the trenches, Scott will provide a database auditing tutorial designed for a business audience</p>	
Target Audience:	
<p>This presentation was written with auditors and IT security professionals of all experience levels in mind. It will provide audit insights for the IT professional and help auditors appreciate the challenges associated with activity monitoring and documentation.</p>	
COBIT Objectives:	
<p>PO9, AI 1,6,7 DS5,9,11 ME1-4</p>	
Speaker Bio:	
<p>Scott Hayes is one of only 60 people in the world to have demonstrated the skills and expertise necessary to be accepted into the elite IBM Gold Consultant program. He is a well known database security and performance expert and a frequent speaker at database trade shows around the globe. ISACA chapters in Tampa, Louisville, Cincinnati, Austin, Columbus, Milwaukee, Chicago, and other cities have asked Scott to give his Database Auditing for Compliance & Security presentation. He holds one US Patent and has others pending for database auditing and performance management solutions and is widely published in various industry magazines. Scott is President, CEO, and founder of Database-Brothers Inc. (DBI), a company focused on helping organizations address database compliance, audit, and security challenges in addition to providing database performance and analytics solutions and consulting.</p>	



Session #C32

Presenter:	Vanessa Balogh
Presentation Title:	Intro to ERP Auditing
Abstract:	Present the challenges that multiple ERP applications and Systems present in regard of the management of SOX regulations and how to master a successful Cross Company and Cross System Audit. Present SAP's Governance Risk and Control Tools as an example for how to support ongoing Governance within a company.
Target Audience:	
COBIT Objectives:	
Speaker Bio:	<p>Vanessa Balogh started her SAP career as a Consultant with SPV AG, Germany from 1991 to 1999. In 1999 she became a partner and founded the US subsidiary SPV America Inc. As the President and CEO she is expanding SPV's SAP business within the US working on Business Development and Client relationships while focusing on Governance, Risk and Control. Following the 25 year old SPV Philosophy of being on the edge of technology and SAP's constant development through dedication of 50 % time to projects work, Vanessa Balogh has lent her diverse Finance, Security and GRC skills to a wide range of national and international SPV clients.</p> <p>Vanessa has written various publications as a journalist and holds several public presentations annually. She studied Communications Science in Vienna, Austria and BA in Munich, Germany. She is member of the IFJ, International Federation of Journalists.</p>

Session #C33

Presenters:	Rudy Chavez, Karl Bledsoe
Presentation Title:	Introduction to Computer Assisted Auditing Tools
Abstract:	<ul style="list-style-type: none"> • Data Analytics Overview – Value to Internal and External Audits • JE CAAT Primer – Value, Techniques and Key Metrics • AR CAAT Primer – Value, Techniques and Key Metrics • Common Tools and Approaches
Target Audience:	<ul style="list-style-type: none"> • Skill level – Beginner & Intermediate • Occupation – Audit, Application development/support personnel, Internal Audit / SOX • Occupational Experience – All
COBIT Objectives:	<ul style="list-style-type: none"> • DS5 • DS11
Speaker Bio:	<p>Rudy Chavez is a Manager in Ernst & Young's San Francisco office within the Risk Advisory Services Practice (RAS). Rudy has over six years experience leading large international projects including SOX advisory services, Integrated Audits, and Data Analytics initiatives. Rudy has extensive experience serving the high tech, manufacturing and defense contractor industries in the Pacific North West. Rudy serves as the area Data Analytics Champion within Ernst & Young's Pacific North West region which includes training, quality and business development responsibilities. Rudy holds a CISA certification from ISACA. Rudy has a BS degree in Accounting from San Diego State University.</p> <p>Karl Bledsoe is a Senior in Ernst and Young's San Francisco office within the Risk Advisory Services Practice (RAS). Karl has over 4 years of experience working on large Integrated Audit, SAS70, and SOX Advisory Service engagements, leading Journal Entry Data Analytic projects, Global Application Control assessments, Procure to Pay Process improvement projects, and IT General control assessments. Karl holds a CISA certification from ISACA and has a BS degree in Management Information Systems from the University of Texas.</p>



Session #G11

Presenter:	Brett Curran
Presentation Title:	Project Risk Management
Abstract:	
In this presentation, Axentis Director of GRC and Privacy Practices, Brett Curran, will explore governance principles and techniques that go beyond simple compliance. He will outline the need for organizations to implement a consistent operational approach to GRC management; an approach that reaches across organizational and functional boundaries, to integrate seamlessly throughout the fabric of the enterprise. Only through an integrated GRC approach will organizations reduce operational redundancy, improve efficiency, enhance transparency and provide for ongoing organizational change management.	
Target Audience:	
Intermediate: Audit, Compliance, Risk and Governance Professionals	
COBIT Objectives:	
Speaker Bio:	
Brett Curran brings a wealth of experience in integrating governance and compliance processes and technology. He has held top information technology management roles at AEGON, Inc. and served as the Director of Imaging and Electronic Workflow at Insurdata. More recently, Brett was the Chief Compliance Officer responsible for enterprise compliance at UICI, Inc. where he established a matrix compliance organization, processes and applied technology to address a myriad of legal, regulatory and operational requirements using a repeatable model. Earlier, he held a variety of technical and project management positions designing, developing and integrating sophisticated technological solutions to simplify and streamline complex business issues.	

Session #G12

Presenter:	Kendall Tieck																								
Presentation Title:	Leveraging CobiT to Audit IT Governance																								
Abstract:																									
<p>Developing an audit approach to IT Governance can be a daunting task. IT Governance is a broad, and often complex business activity that many IT auditors cite as control concern, but often fail to include in the audit plan. The IT Governance challenge often takes many experienced technology auditors out of their IT comfort zone. By leveraging CobiT 4.0 the foundation for an audit approach can be developed and reduce the complexity and mystery of auditing IT Governance.</p>																									
Target Audience:																									
<p>Audit Professionals seeking to define an audit approach to IT Governance. Seniors, Managers and Directors may find the content appropriate for relevant activities.</p>																									
COBIT Objectives:																									
<p>All CobiT Domain will be addressed, but the following will be highlighted:</p> <table border="1"> <tr> <td>PO 1</td> <td>Define a strategic plan</td> </tr> <tr> <td>PO 2</td> <td>Define the information architecture</td> </tr> <tr> <td>PO 3</td> <td>Determine technological direction</td> </tr> <tr> <td>PO 5</td> <td>Manage the IT investment</td> </tr> <tr> <td>PO 6</td> <td>Communicate management aims and direction</td> </tr> <tr> <td>PO 9</td> <td>Assess and manage IT risks</td> </tr> <tr> <td>DS 1</td> <td>Define and manage service levels</td> </tr> <tr> <td>DS 6</td> <td>Identify and allocate costs</td> </tr> <tr> <td>ME 1</td> <td>Monitor and evaluate IT performance</td> </tr> <tr> <td>ME 2</td> <td>Monitor and evaluate internal control</td> </tr> <tr> <td>ME 3</td> <td>Ensure regulatory compliance</td> </tr> <tr> <td>ME 4</td> <td>Provide IT governance</td> </tr> </table>		PO 1	Define a strategic plan	PO 2	Define the information architecture	PO 3	Determine technological direction	PO 5	Manage the IT investment	PO 6	Communicate management aims and direction	PO 9	Assess and manage IT risks	DS 1	Define and manage service levels	DS 6	Identify and allocate costs	ME 1	Monitor and evaluate IT performance	ME 2	Monitor and evaluate internal control	ME 3	Ensure regulatory compliance	ME 4	Provide IT governance
PO 1	Define a strategic plan																								
PO 2	Define the information architecture																								
PO 3	Determine technological direction																								
PO 5	Manage the IT investment																								
PO 6	Communicate management aims and direction																								
PO 9	Assess and manage IT risks																								
DS 1	Define and manage service levels																								
DS 6	Identify and allocate costs																								
ME 1	Monitor and evaluate IT performance																								
ME 2	Monitor and evaluate internal control																								
ME 3	Ensure regulatory compliance																								
ME 4	Provide IT governance																								
Speaker Bio:																									



Kendall Tieck is hold the position of Audit Director at Microsoft Corporation in Redmond, Washington. His is responsible for developing and executing the internal audit strategy for the Microsoft Business Groups, specifically the Platforms & Services Division, Entertainment & Devices, and Microsoft Business Division. Together, these groups produce the products and services that address a variety of markets from consumer to commercial, from gaming to mission critical business platforms.

Previously at Microsoft, Kendall was the IT Group Manager and was responsible for audit covered of Microsoft technology infrastructure globally, including networks, data centers and key IT enterprise processes.

Kendall has over 20 years of experience in technology and audit. He has managed technology in several departments including the Real Estate Industries Group and Audit Division of Wells Fargo Bank. Kendall served as MIS Director for a software publisher, Theatrix Interactive, Inc., a publisher of dual platform, multimedia educational software. As a technology manager, Kendall led the introduction of new technologies in several key businesses.

As an audit professional, Kendall worked for Wells Fargo Bank, Bank of America and Microsoft. His areas of expertise include risk management, distributed technologies, networks, data centers and information security. Over the span of his audit career, Kendall has been involved in several major business initiatives including technology outsourcing, merger/acquisition transitions, major systems conversions and enterprise technology initiatives. Prior to joining Microsoft, Kendall was an SVP in the Technology Risk Management, Technology and Operations Division. Kendall has been a guest speaker at local and national ISACA events and has taught seminars on control and security of distributed technologies.

Session #G13

Presenter:	Yong-Gon Chon
Presentation Title:	Security Effectiveness Metrics - Creating a Compelling Business Case
Abstract:	
<p>Today's Information Security Leaders are facing more pressure to demonstrate the effectiveness of their programs from business owners, regulators, and from internal and external customers. How does your organization value your contributions to the bottom line if <i>NOTHING</i> happens when you're doing your job well? No incidents...\$0. No viruses...\$0. Staying off the evening news because you didn't suffer a privacy compromise...PRICELESS. In this session, we will explore the various metrics that Fortune 500 companies and Federal Agencies use to tell a compelling security story. We will show you how to use these metrics to support your business case that will allow your organization to operate without concern. This session will help enable you to evolve your security program by integrating a business value message into every security project.</p> <p>The participant will learn more about:</p> <ul style="list-style-type: none"> • Security metrics being used in the public and private sector today • Quantifying your security program's effectiveness • How to build security value chains into the business • Strategies for proving the elusive Return on Security Investment (ROSI) <p>Session Objectives: Provide an understanding of how and why programs security programs fail, using metrics to support security initiatives, reporting success, benchmarks across the industry.</p> <p>Skills Learned: You will learn how to more effectively use security metrics to build business cases for your initiatives. Additionally, you will be able to reflect on your current organization's metrics against the collective experiences of Fortune 500 organizations and Federal agencies.</p> <p>Applying this session: You will be able to build more effective security business cases by quantifying success and relating results more effectively to your core business.</p>	
Target Audience:	
Target audience: Chief Security Officers, Information Security Leadership, Experienced Security Professionals responsible for justifying security spending.	
COBIT Objectives:	
DS1,2,3,5,6,7 PO1,5,9 ME2,3	
Speaker Bio:	
<p>Mr. Chon is an Information Security Subject Matter Expert for over 14 years and has helped Federal Agencies and Fortune 1000 customers with build effective security programs and demonstrate compliance to FISMA, ISO17799, SOX, GLBA, NERC, HIPAA and PCI. Mr. Chon has appeared on CNN, MSNBC, ABC, and Fox News as a security expert on topics such as Mobile Computing Viruses, Denial of Service Attacks, and Vulnerability Intelligence. Mr. Chon received Forbes Magazine whitepaper of the week honors for "Justifying Security Spending" and wrote the Information Security Magazine cover story, "Wide Open on Port 80." As an adjunct professor at the George Washington University, he was responsible for leading UNIX and TCP/IP courses and mentoring other instructors on the security aspects of course materials. As SecureInfo's Senior Vice President of Services, Mr. Chon is responsible for driving the strategy and direction for SecureInfo's services line of business. Previously, Mr. Chon was Director of Compliance at Cybertrust, where he drove the company's strategy for compliance products and services. Prior to the formation of Cybertrust, Mr. Chon was Director of Consulting at TruSecure. At TruSecure, Mr. Chon developed a world-class professional security services organization from grass roots to global delivery and developed the first application security certification based on continuous essential practices.</p>	



Session #G21

Presenter:	Gerald Meyers
Presentation Title:	Leveraging IT Audit Resources – IT Risk Assessment Through High-Impact Audits
Abstract:	This session is designed to give the participant an overview into IT Risk Assessment Methodology and Approach through the development of an Audit Plan. In addition, there is discussion around what a high-impact IT Audit plan might consist of including what to consider when deploying.
Target Audience:	
COBIT Objectives:	
Speaker Bio:	<p>I am a Senior Manager in Protiviti's Santa Clara office Technology Risk Practice. My background includes extensive experience in information technology risk assessments focusing on access and data-integrity control issues, Unix, AS/400 and application level security reviews, and assessments of IT policies and procedures. I have over eleven years of total technology experience including more than nine years in internal / external technology audit and controls assessment. This includes 3 years with Arthur Andersen, 2 years at Deloitte & Touche, and over 3 years with Protiviti. Before joining public accounting, I worked for over a year with Hughes Supply as an Internal IT Auditor, and two years as a database administrator for both USAir and the Sanford Airport Authority.</p> <p>I specialize in our IT Audit Services (ITAS) practice line and am part of Protiviti's national team. I actively participate in teaching at both the local and national levels. Each year I develop / deliver between 3 to 8 training programs ranging. Examples from the past 12 months are:</p> <ul style="list-style-type: none">• IT Audit Essentials – Developed and Taught• IT Risk Assessment Basics – Developed and Taught• Workpaper Documentation Essentials - Taught• Internal Audit Leadership School - Taught• New Senior School - Taught• Leveraging Compliance for Operational Efficiency – Moderated Panel Discussion (IIA / ISACA Joint Meeting)• Compliance Best Practices – Moderated Panel Discussion (ISACA) <p>Along with my Protiviti responsibilities, I am an active member of the local ISACA and IIA chapters and am the Education Committee Chairman for ISACA Silicon Valley. I have been an ISACA Board Member 2 previous times.</p>



Session #G22

Presenters:	Slalom Consulting - Gary Ross, CA, CISA and Scott Perry, CPA, CISA
Presentation Title:	Enterprise Risk Management and IT's Role
Abstract:	
Session will provide an overview of Enterprise Risk Management and IT's role in the process. Attendees will learn about ERM goals, frameworks and approaches, how IT can integrate into the ERM process and drive value to the business and in some cases be a primary driver for ERM in the organization. Attendees will come away with a better understanding of ERM programs in their organizations and how they can engage.	
Target Audience:	
Session is targeted at intermediate to advanced financial/operational auditors, IT audit or IT risk management professionals at the manager level and above who are involved in risk management activities, internal audit or who are considering an enterprise risk management program.	
COBIT Objectives:	
PO1, 4 and 9 ME2, 3 and 4	
Speaker Bio:	
Scott Perry, CPA, CISA Scott is the National Director of Enterprise Quality & Compliance Solutions for Slalom Consulting. Scott has over 20 years of professional services experience as a CPA, IT Audit Professional and Project and Program Manager. Formerly with Big Four firms Ernst & Young and Deloitte & Touche, Scott performed IT general and application control assessments (including security policies, practices and operations) for over 100 companies including, Boeing, Microsoft, PacifiCorp, Alaska Airlines, Amazon and Paccar.	
Gary Ross, CA, CISA Gary leads the Enterprise Quality & Compliance Solutions team in the San Francisco Bay area. He has over 17 years of professional experience as a senior IT and financial auditor and has worked with clients in retail, healthcare and financial services. Gary is a former VP of Internal Audit for Williams Sonoma and a former KPMG Information Risk Management Director. Gary has led teams providing IT audit and security services to many large Fortune 500 clients including Gap Inc, Ross Stores, Trader Joes, Blue Shield of California and Wells Fargo.	

Session # G23

Presenter:	Stephen Spalding
Presentation Title:	Beyond SOX; The High Value Audit
Abstract:	
<p>This is an interactive discussion on “What are the aspects of a High Value Audit” in an organization, which SOX is no longer the center of focus. As such, the following points will be covered:</p> <ul style="list-style-type: none"> • Define “Value” from the Audit Committee prospective. • Consider what a risk model might like from the Audit Committee prospective, which maybe different that the classic business risk models. • Discuss Internal Audit’s changing relationship to SOX 	
Target Audience:	
<p>Anyone interested in the changing value expectations on the Internal Audit functions. Primarily, this would include:</p> <ul style="list-style-type: none"> • Current/future Internal Audit Management Team members • Risk management and compliance personnel • SOX project administrators and related personnel 	
COBIT Objectives:	
<p>Speaker Bio:</p> <p>Stephen Spalding, Principal at Grant Thornton, LLP, is the Practice Leader for the BAS (Business Advisor Services) practice in the Bay Area which provides services related to information security, SAS70 reporting, internal audit, SOX compliance and internal control design/development.</p> <p>Prior to joining Grant Thornton, Stephen was the CEO of Vigilant Privacy Corporation which focused on providing enterprise technology solutions supporting a wide range of legal and compliance requirements, including Sarbanes-Oxley and HIPAA.</p> <p>Stephen has eighteen years of working experience in the “Big 4”, eleven of these as a Partner. In Deloitte, he developed the Bay-Area Enterprise Risk Services practice which included Internal Audit Services, Technology Control Assurance, Data Quality and Project Risk Management. He was one of the three founding partners of KPMG’s Information Risk Management practice. Prior to that, Stephen also established Internal IT Audit functions at two Fortune 100 companies.</p> <p>Stephen is currently also an instructor at San Francisco State University, where he teaches Internal Audit and Business Systems Management and Control at the Senior/Graduate Level. He holds an MBA in Quantitative Analysis from the University of Arizona, and B.S. degrees in Finance and Management, Physics (solid state) and Mathematics, from Eastern Illinois University.</p>	

Session #G24

Presenter:	Jackson Willett, MBA, CISA
Presentation Title:	How to effectively audit a Project Management Office (PMO)
Abstract:	
<p>This course designed to provide a high-level overview of how Internal Auditors can approach audit to a Project Management Office that has oversight and risk mitigation responsibilities for a strategic initiative. It will:</p> <ul style="list-style-type: none"> • Define a Project Management Office and the different types of structures as well as risk responsibilities to drive a strategic initiative to success • What should Internal Audit's role be if any in a PMO • What should be the key audit objectives to perform a PMO review • What constitutes an effective PMO and what are the "red flags" to an auditor • Internal Audit's value proposition to executive management for reviewing a PMO 	
Target Audience:	
<p>Anyone interested in gaining a better understanding of what is a Project Management Office and how can Internal Audit add value to a key initiative's success:</p> <ul style="list-style-type: none"> • Internal Auditors • Project Stakeholders • Project sponsors 	
COBIT Objectives:	
CoBIT does call for proper project management over system development/integration.	
Speaker Bio:	
<p>Jackson has over 18 years of experience in both industry and professional services delivery. Recent experience includes project management leadership during all phases of Sarbanes-Oxley ("SOX") compliance projects for several large cap companies. In addition, Jackson has worked with clients to implement Application and General Computing Controls, Business Process Improvement and IT Governance solutions to strengthen process and control activities identified as a result of SOX findings. Jackson's recent industry experience includes consumer products, aerospace & defense, manufacturing/distribution and insurance clients. Jackson possesses solid analytical and project management skills with demonstrated success in delivering complex projects within limited timeframes and budget.</p>	

Session #G31

Presenter:	David Willoughby
Presentation Title:	Internal Controls Optimization
Abstract:	Defining internal controls optimization - what are the practical aspects of implementing and the elements to consider in optimizing your controls for business benefit.
Target Audience:	Intermediate Audit, Finance, Compliance
COBIT Objectives:	
Speaker Bio:	David Willoughby has over 18 years experience serving clients of PwC. David is a member of the Firm's Systems and Process Assurance practice, focusing on controls related projects, including implementation and maintenance of Sarbanes-Oxley, optimizing control structures and managing systems of controls. He has assisted clients in all facets of implementing Sarbanes-Oxley - project management, scoping, documentation, testing, assessment and optimization of systems of controls - covering all business cycles - financial accounting and reporting, tax, human resources, payroll, revenue, procurement, inventory, fixed assets, Information Systems. He has managed many projects, ranging in size from 2,000 hours to over 24,000 hours. David was also involved with PwC's global task-force to design and develop methodologies and tools to aid clients in designing efficient systems of controls with a focus on optimizing controls structures. David has served an array of clients in the retail, consumer packaged goods, manufacturing, mining, industrial products, technology, not-for-profit, transportation and financial services industries.

Session #G32

Presenter:	Mark Seward
Presentation Title:	"Operationalizing Security and Compliance: Generating Maximum Compliance ROI"
Abstract:	
<p>This is an introductory to intermediate-level course designed to offer tips for integrating the compliance process into current business processes to push aspects of compliance and risk to the business process owners. It will:</p> <ul style="list-style-type: none"> • Discuss the current "as-is" situation regarding the lack of alignment between IT and the rest of the business. • Create an understanding of what are departmental vs. cross-departmental processes. • Define a needs assessment process and approach for determining the needs of the Business and creating alignment and compliance risk acceptance. • Define a "just-in-time" approach for presenting information to the business process owners. • Define the linkage between this new alignment and COBIT CMM model. • Define the relationship to ROI 	
Target Audience:	
<ul style="list-style-type: none"> • Skill Level Beginner to Intermediate • Occupation – Audit, Security, Business process owner • Anyone interested in getting a better understanding of the processes that drive the business and what IT needs to do to support these processes. Also, learn tips for moving the business risk associated with GRC from IT to the business owners. 	
COBIT Objectives:	
<p>This course will introduce all COBIT areas, but will focus on the following: PO 1, 4, 6, 9 ME 3, 4, 1-2</p>	
Speaker Bio:	
<p>Mark Seward, CISA, CISSP Director Product Marketing, Policy Compliance, Qualys</p> <p>Mark is currently Director of Product Marketing for Qualys' QualysGuard Vulnerability Management product and the forthcoming QualysGuard Compliance Module. These responsibilities include product roadmap, messaging, and simplifying compliance and vulnerability management processes.</p> <p>Qualys is the leader in vulnerability management with over 3000 customer subscriptions to its software-as-a-service (SaaS) offering. Mark came to Qualys from Symantec's Managed Security Services (MSS) division where as Senior Product Manager he was in charge of the integration and support roadmap for over 20 products.</p> <p>While with Qualys, Mark has led three four new releases of QualysGuard, expanded the number of third-party integrations with QualysGuard to over twenty-five companies, and expanded the number of APIs available to twenty-seven, This has enabled customers to completely integrate the QualysGuard solution with their own security portals.</p> <p>While at Symantec Managed Security Services he lead and completed an effort to correlate customer supplied network and host IDS/IPS data with Qualys vulnerability data to reduce false-positives and predict attack vectors for malicious activity.</p> <p>Mark has eight years of experience in the information security field in Product Management, as a Security Engineer, and a Technical Product Manager. He has obtained a Clinger-Cohen Federal CIO certification and has an MS in IT from the University of Maryland.</p>	



Session #G33

Presenter:	Terry Nystrom, SVP Field Operations, Prodiance Corporation Dannette Roberts, Industry Partner Manager, Microsoft Corporation
Presentation Title:	End User Computing Controls
Abstract:	
<p>As organizations move forward with SOX 404 and other compliance efforts, an area of high risk remains within the uncontrolled data, complex formulas, and macros contained in financial spreadsheets, access databases and other end user computing documents. Leading tax and audit firms are now recommending EUC controls to reduce the risk of errors in the reporting process, but understanding the risks, conducting an assessment, and finding a sustainable solution to address this problem can be overwhelming at best. Join Terry Nystrom and Dannette Roberts to analyze the use of spreadsheets in the financial reporting process, understand the compliance implications for SOX 404, the critical areas of risk and learn about how to deploy a comprehensive solution. Their presentation will cover:</p> <ul style="list-style-type: none">• The business risks associated with the use of financial spreadsheets and other EUCs• The latest guidance from auditors on key spreadsheet controls for remediation• Best practices for assessment, inventory and implementation• A comprehensive solution framework for sustaining compliance	
Target Audience:	
<p>This presentation will benefit various levels and disciplines involved in the development, use, audit and control of financial spreadsheets and other end user computing documents. Senior financial and IT executives will care about the compliance, visibility and control aspects while internal audit and compliance teams will benefit from knowing that automated tools and processes exist to help them perform their functions.</p>	
COBIT Objectives:	
<p>End user computing has not been subject to control activities within IT or the same development and testing processes. This presentation will describe practices, processes and automated solutions to address this uncontrolled area.</p>	
Speaker Bio:	
<p>Terry Nystrom brings more than 25 years of sales experience to his role of senior vice president, Field Operations for Prodiance. Previously, Terry held senior management positions at a number of leading enterprise solution providers delivering content and compliance solutions to global organizations.</p> <p>Dannette Roberts brings over 20 years of experience in the Retail Banking vertical concentrating in areas such as Solution Selling, channel management, sales management and technical roles. As Industry Partner Manager for Microsoft she is familiar with the issues of end user computing and supports Microsoft customers and field organization by providing solutions to assist them in the control and management of their end user computing environment.</p>	

Session #S11

Presenter:	Mike Shema
Presentation Title:	Web Application Security: Finding Vulnerabilities in Dynamic Applications
Abstract:	
<p>In 2006 web applications received more attention in terms of publicly reported vulnerabilities. Exploits for those vulnerabilities also increased in sophistication and purpose. Web sites tend to include more technologies that provide dynamic interactions between the browser and the application. This increases their exposure to vulnerabilities in functional and business logic.</p> <p>Web application owners and security auditors must continue to find and reduce vulnerabilities due to input validation and data storage. Yet the growth of client-side functionality placed in JavaScript or browser plug-ins like Flash or ActiveX means that even more care must be taken when reviewing the business logic and program flow of an application. If an exploit is able to take advantage of a web browser's implied trust of the application, then the user's data can be compromised or the web browser can be used to propagate a worm across the application. Both scenarios can have a significant impact on the web site.</p> <p>This presentation will summarize some web application worms and how they combined input validation exploits (e.g. Cross-Site Scripting) with dynamic content in order to exploit the logic of a web application. It will include examples of vulnerabilities that arise from increased reliance on client-side engines. The presentation will also highlight the need to increase the security of desktops and web browsers in order to protect users from a compromised or malicious web application.</p>	
Target Audience:	
<p>Attendees should be familiar with web-related technologies, but detailed understanding of items such as AJAX and DOM is not necessary as these will be explained in the context of threats and vulnerabilities.</p> <p>Attendees who are concerned with web application security will gain more insight into the evolution and sophistication of attacks; those who are concerned with desktop security and data theft will gain an understanding of how malicious web sites can be used to attack users.</p>	
COBIT Objectives:	
Speaker Bio:	
<p>Mike Shema is the co-author of Hacking Exposed: Web Applications, The Anti-Hacker Toolkit, and the author of Hack Notes: Web Application Security. He has extensive consulting experience with information security within a variety of industries. While his security background ranges across network penetration testing, wireless auditing, code review, and training, he primarily focuses on web application security. He currently works at Qualys, developing tools that automate the web application audit process.</p>	

Session #S12

Presenter:	Aaron Weller
Presentation Title:	Information Leak Prevention – How to Tame the Insider Threat
Abstract:	
<p>This session describes the many types of Information Leakage, how they can take place and what is at risk. By looking at information as an important company asset, and identifying who might benefit from access to it, I will describe some of the ways that information is leaking out of almost every organization today. From looking at the problem, I move to describing recent developments in the space of managing information leakage, both across the network and at the desktop and on end-user devices. Examples from current information leak prevention technology will be used to show the benefits, and some limitations of the current state of the art. Participants will benefit from an explanation of what they can do to improve their controls over information leakage within their own organization, and how they can increase the maturity of their processes in this area.</p> <p>The participant in this session will learn about:</p> <ul style="list-style-type: none"> ○ What is at stake? – examples of information leakage in the news ○ How to identify the information you need to protect ○ Overview of the market for solutions and the major features of available tools ○ Examples of actual findings ○ What next? Steps you should consider to address this issue. 	
Target Audience:	
<p>Skill Level: Beginner Occupation: Audit / Security / Legal Occupational Experience: Any – different levels will get different things out of this presentation</p>	
COBIT Objectives:	
<p>P05 – Manage the IT Investment P09 – Assess and Manage IT Risks DS5 – Ensure System Security DS9 – Manage the Configuration</p>	
Speaker Bio:	
<p>Please provide a brief, one paragraph description of your background, emphasizing your knowledge and experience with your topic.</p> <p>Aaron is the leader of Protiviti's Northern California security practice. He has a decade of professional risk management experience, including time spent working for a number of the Big 4 auditing and consulting firms. Aaron is a Certified Information Systems Auditor (CISA) and a Certified Information Security Manager (CISM). Aaron has been a member of ISACA since the 20th century, and was the secretary to the board of the Melbourne, Australia Chapter from 2004-2006.</p> <p>Aaron has been based in the UK, Australia and the USA during his career, which brings an international perspective to his work. He has performed IT line management roles as well as auditing / consulting, giving him a perspective on how to develop pragmatic solutions to address risk.</p> <p>Aaron is currently involved in a wide variety of initiatives, including taking on interim CISO roles for clients. His current focus is improving the maturity of security processes.</p>	

Session #S13

Presenters:	Erik Jonte, Brad Ames, Jessica Amezcuita
Presentation Title:	Continuous Monitoring for IT Audit
Abstract:	
<p>Continuous Control Monitoring (CCM) is a strategy to align indicators in IT General Controls and configurable application controls in order to gain a portfolio view of emerging risk across functions and business units. By benchmarking automated controls, the model provides assurance and isolates outliers for the purpose of deploying audit resources to risk that matters most. This session will discuss two experiences in Google Inc. and the Hewlett-Packard Company where the CCM benchmarking strategy is paying off. The segment, led by IT audit practitioners, will explain how the CCM techniques are accomplished through internal audit engagements.</p> <p>This course is focused on the use of automated and continuous methods for assessing IT compliance. The topics discussed will include strategies for gaining access to underlying data, techniques for processing the information into useful metrics / indicators, and how to integrate this new approach into an existing audit methodology. Attendees will gain an appreciation for the value of a continuous approach and will be armed with a list of resources that they can use to apply the techniques to their own departments.</p>	
Target Audience:	
<p>Skill level – Intermediate to Advanced Occupation: Audit / Security Experience: Senior to Manager</p>	
COBIT Objectives:	
<p>AI6, AI7, DS1, DS3, DS5, ME1, ME2, ME3,</p>	
Speaker Bio:	
<p>Erik Jonte Mr. Jonte has over 5 years of experience in the Information Security and IT Audit disciplines. He has audited and consulted with over a dozen companies in Silicon Valley, and has held positions with Ernst & Young, eBay, and Google. In addition, he has spent much of his tenure at Google developing automation strategies to improve the accuracy and efficiency of IT internal audit.</p> <p>Brad Ames, CPA, CISA Ames is the Internal Audit SOX Director for the Hewlett-Packard Company in Palo Alto, California. Prior to joining HP in 2000, he was an Audit Manager for Transamerica Corporation and previously Computer Assurance Services Manager with Coopers & Lybrand LLP, in Los Angeles.</p> <p>Brad's team is responsible for developing audit solutions and innovations for the purpose of measuring emerging risk in connection with application systems reliability, data center operations, and implementation projects. Brad directs the Sarbanes-Oxley (SOX) 404 Attestation effort on behalf of Internal Audit and works closely with HP's Enterprise Compliance Group. His role involves close collaboration with IT governance groups, customers and external auditors in order to gain an ongoing view of IT risk enterprise-wide. He is currently advancing continuous control modeling and measurement for the purpose of simplifying SOX 404 attestation.</p> <p>Brad is a CPA and Certified Information System Auditor with 10 years of experience in Public Accounting. He can be reached at brad.ames@hp.com.</p> <p>Jessica Amezcuita, CPA Jessica is an Internal Audit Manager who joined Hewlett-Packard Internal Audit as an IT auditor in 2004 after working in public accounting. She has a degree in Economics from University of California, Santa Cruz and a graduate degree in Accounting from University of Texas, Austin. Jessica speaks Spanish and enjoys snowboarding, camping, cooking, hiking, enjoying nature, and spending time with family and friends.</p>	

Session #S21

Name:	Michael Smith
Presentation Title:	How to Protect from Malicious Code – Using Honeynet and Darknet Technology as Part of a Compliance Program
Abstract:	
<p>The purpose of this presentation is to explain and demonstrate methods for improving an organizations' security posture as it is related to untargeted malicious code. I will show why this is important and how measurable success can be achieved with minimal resource investment. The specific methods that I will be examining are the creation of an Incident Response (IR) toolkit and the deployment of a honey net and/or dark net.</p> <p>The participant will learn more about:</p> <ul style="list-style-type: none"> • The importance of Configuration Management (CM) and sound engineering practices to security • The ways that honey net technologies could be valuable to your organization and how they can be a part of a greater compliance solution • How to detect possible malicious code on your network • What to do if you discover malicious code on your network 	
Target Audience:	
<p>Intermediate-Advanced Security First line managers and direct contributors</p>	
COBIT Objectives:	
<p>DS3 Manage Performance and Capacity DS5 Ensure Systems Security ME1 Monitor and Evaluate IT Processes ME2 Monitor and Evaluate Internal Control</p>	
Speaker Bio:	
<p>Mr. Smith has more than ten years of experience in the field of Information Security. He has provided security consulting services to state, local, and federal governments as well as many commercial clients across multiple verticals. He has achieved various industry certifications throughout his career, such as the PMP and CISSP. He has published articles about honeynet and darknet technologies and is currently doing research related to malicious code detection. Most recently Mr. Smith has worked as the Senior Manager to design and manage the operation of the Multi-Sate Information Sharing and Analysis Center Security Operations Center (MS-ISAC SOC).</p>	



Session #S22

Presenter:	Rodney Kocot
Presentation Title:	Security - A System Settings Perspective
Abstract:	
<p>This session provides an overview of system settings that must be reviewed in order to provide an opinion regarding the level of security implemented on a system. A method for determining the scope of a review and an approach for obtaining the necessary information will be discussed. A process for identifying system settings will be explained. System settings for several operating systems will be discussed. Examples of obtaining and reviewing information will be shown.</p>	
Target Audience:	
<p>Session materials and session discussions are beneficial to all skill levels. IT Auditors and Security Administrators will receive information that will enable them to perform more effective, efficient and detailed reviews of system security.</p>	
COBIT Objectives:	
Speaker Bio:	
<p>SPEAKER: Rodney Kocot, Systems Control and Security Incorporated</p> <p>Rodney Kocot is a technical IS Audit Consultant for Systems Control and Security Incorporated. Rodney provides technical audit training and consulting services for corporations worldwide. He has been an IS Auditor for 23 years with responsibilities that included technical audits of operating systems, network audits, and audit software development.</p> <p>Rodney often presents at the ISACA CACS and International conferences. He has presented numerous seminars and dinner meetings all over the world for the last 23 years. Seminars presented by Rodney include automation techniques, software, and audit programs. Topics include programming, audit and security automation, auditing minicomputers, and securing minicomputers. He has performed AS/400, LAN, Tandem Guardian, Unisys, Unix and OpenVMS audits using Visual Basic and Microsoft Access to automate the reviews.</p> <p>Rodney has been working with and programming PCs since 1982 using CPM. He currently programs mostly with Visual Basic, but also knows C++ and other languages. He has been working with Windows since its inception.</p> <p>Rodney has been involved in the Information Systems Audit and Control Association, and has held various positions in the Los Angeles and San Francisco chapters including President, Executive Vice President, Vice President, and Secretary.</p>	

Session #S23

Presenter:	Jeffrey Camiel
Presentation Title:	Wireless Systems Vulnerabilities, Threats, and Auditing
Abstract:	
<p>Wireless networks are replacing traditional hardwired networks and growing the number of endpoints at extreme rates. There is the standard wireless of the standard access point, but are you assessing the risk around wireless mobile systems, around wireless keyboards, Bluetooth networks, adhoc mesh-networks, wireless network bridges? As an IT auditor, it is your job to assess the threats and vulnerabilities related to wireless systems and architectures and explain the risks to management. To be able to do this, the auditor needs to understand the tools that are used and the methodology used by intruders used to “crack” wireless systems. This session will provide:</p> <ul style="list-style-type: none"> • Live demonstrations of the threats and vulnerabilities related to 802.11 (WI-FI) and Bluetooth. • Demonstration of open source tools to detect and find weaknesses in wireless systems • Walkthrough of IT a wireless audit program. 	
Target Audience:	
<p>Skill level – Beginner, Intermediate and advanced Occupation – Audit, Security Occupational – All Levels</p>	
COBIT Objectives:	
<p>Monitor and Evaluate ME2 ME3</p>	
Speaker Bio:	
<p>Jeffrey has 20 years experience managing and performing IS audits, security assessments (penetration testing and vulnerability assessments), compliance assessments, operational audits, and secure network design in the high tech, financial, insurance, and pharmaceutical industries. Jeffrey specializes in large network, application penetration and vulnerability assessments, and privacy and compliance readiness. Jeff has developed and managed technology security research and education labs for various consulting firms. Jeff is the Director of Technology Risk Management for Jefferson Wells and manages the Technology Risk Research and Education Center.</p>	

Session #S24

Presenter:	Mark S. Kadrich
Presentation Title:	Endpoint Security
Abstract:	
<p>There are systems on your network that you don't control. When did the vending machines become a vector for a network attack? Why can't I trust my printer? Besides the standard Windows, Mac, and Linux systems, I will discuss the security issues of various types of systems ranging from handhelds to embedded control systems. Virtually everything is getting a network connect these days and sometimes, many times, that's a bad thing. We will discuss what type of controls are available and how a process control model can be used to ensure system trust - and how some systems just can't be trusted. I will discuss how the endpoint and the network must work together to ensure compliance and security because by themselves they are not capable of making an accurate determination.</p> <p>The participant will learn more about:</p> <ul style="list-style-type: none"> ↑ Hidden network threats ↑ NAC (the many flavors) ↑ Embedded systems ↑ A new way to address network control ↑ Trust based control architecture 	
Target Audience:	
<p>All skill levels Audit, Security</p>	
COBIT Objectives:	
<p>The proposed solution concept maps directly to COBIT control objectives in multiple dimensions.</p>	
Speaker Bio:	
<p>Mark S. Kadrich – CISSP - The Security Consortium, Inc For the past 20 year Mark Kadrich has been a contributing member of the security community. His strengths are in systems level design, policy generation, end point security, and risk management. His book Endpoint Security (Addison Wesley) is available now. Mr. Kadrich is presently President and CEO of The Security Consortium, whose mission is to provide complete security product knowledge to their customers. TSC performs in-depth testing and evaluation of security products and the vendors that provide them. Prior to TSC, Mr. Kadrich was Senior Manager of Network and Endpoint Security for Symantec. His role was to ensure that the Symantec business units correctly interpreted security policy during their pursuit of innovative technology solutions. Mr. Kadrich was senior scientist with Sygate Technologies prior to the Symantec acquisition. Mr. Kadrich joined Sygate through the acquisition of a start-up company where he was a founding member.</p>	



Session #S31

Presenter:	Ravi Jagannathan
Presentation Title:	Locating Sensitive Data in Structured Data Sets
Abstract:	
<p>The need to secure corporate sensitive data has never been greater. A number of compliance laws and standards such as Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry Data Security Standards (PCI DSS), etc. are driving corporations towards adopting robust processes for ensuring the security of sensitive data. This session will look at a systematic approach to locating sensitive data in structured data sets and how it enables a repeatable process of compliance audits to ensure proactive control.</p> <p>The participant will learn more about:</p> <ul style="list-style-type: none">• The key elements of Sensitive Data security• A framework and a 3-phase approach to methodically locate sensitive data in structured data sets• Why it is important to use a “best practice” framework for sensitive data discovery	
Target Audience:	
Skill Level – Beginner, Intermediate Occupation – Audit, Security, Data Management	
COBIT Objectives:	
Speaker Bio:	
<p>Ravi Jagannathan is Senior Director of Technology at Exeros, Inc., a data relationship discovery company. He has 20 years of experience in systems, data integration and analytics application software design, development, product strategy and management and deployment functions at companies including Digital Equipment, Oracle, Broadbase, Acta Technology and Tradec/Agile. His education includes dual master degrees in Computer Engineering and Operations Research from Rensselaer Polytechnic Institute (RPI) in Troy, NY. At Exeros, Mr. Jagannathan is responsible for creating methodologies and solutions and driving the adoption of Exeros’s unique discovery technology in key areas of Data Governance such as Sensitive Data Discovery and Master Data Management (MDM).</p>	



Session #S32

Presenter:	Scott Smith
Presentation Title:	Data Privacy – Protection From Trusted Users
Abstract:	
<p>How do you protect against sensitive data breaches where users are authorized to access the data?</p> <p>In this session, we will examine several areas where sensitive data that is accessible by “authorized users” presents a security risk, and explore how companies can reduce the risk that data is misused or exposed by trusted users.</p> <p>In the first portion of this session, we will discuss IT’s use of sensitive data for developing and testing software applications and how companies can take measures to safeguard that data. While organizations may think that test data is immune from privacy threats, these environments are less secure and may be exposed to a variety of unauthorized sources; including in-house QA testing staff, consultants, partners, and offshore development and support personnel. We will discuss how to implement a comprehensive Test Data Solution that involves a combination of best practices, processes, technology, and expertise to effectively protect data.</p> <p>In the second half of this session, we will examine how to protect against data breaches caused by trusted insiders who <i>have</i> authorized access. Study after study reveals that the biggest security threat organizations face is internal. Utilizing an advanced “surveillance camera” technology, companies can record authorized internal activity between users and mainframe based applications with full audit trails. If a data breach occurs auditors can quickly pinpoint what data is compromised. Just the knowledge among users that this type technology is employed is a deterrent.</p>	
Target Audience:	
Target audience is Auditors and Security managers and executives	
COBIT Objectives:	
Speaker Bio:	
<p>Scott Smith has over ten years of experience in the Information Technology business supporting the development, sales, and implementation of software solutions, mission critical business applications, and consulting services for many Fortune 1000 companies. Throughout his career with Compuware Corporation, Mr. Smith has been highly successful at implementing enterprise-wide Data Privacy solutions by providing leadership in the deployment of technology and best practices to assist customers in lowering the risk of exposure, cost of regulatory compliance, and optimizing productivity in many Data Privacy initiatives for financial, health care, and government industries. Mr. Smith holds a B.S. degree in Computer Science and Business Administration from Fitchburg State College in Fitchburg, MA.</p>	



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>	



Session #T1

Presenter:	Donald E. Hester
Presentation Title:	Security Features of Windows Vista
Abstract:	Security features/improvements to in Microsoft Windows Vista. What's new? What's under the hood? Learn why you want Windows Vista as soon as possible. Learn about Vista's malware protection, integrity controls, changes to user accounts and authentication. Learn about Vista's data protection capabilities including EFS, BitLocker, and RMS. Learn about Windows Vista's network protection features. Learn about Vista's increased audit capabilities and improved error management and performance tracking.
Target Audience:	All levels
COBIT Objectives:	At least PO9, AI1, AI6, DS3, DS4, DS5, DS9, DS11, & ME1
Speaker Bio:	Donald is the Information Systems & Security Manager, consultant, and auditor for Maze & Associates. His clients include local municipalities, non-profits and federal government agencies, specializing in a wide array of compliance programs such as PCI, FISMA, COBIT and ISO17799. He is a Guest lecturer and speaker on security topics. Donald received his bachelors, with honors, in Security Management with a concentration in Information Security from American Military University. His certifications include; CISSP, CAP, CISA, MCT, MCSE Security, MCSA Security, MCDST, Security+ and CTT+. Donald also teaches at San Diego City College and for the California State Chancellor's office.



Session #T2

Presenters:	Derek Koopowitz, Norm Gutierrez, Rob McIndoe – California State Automobile Association (AAA Northern California)
Presentation Title:	Infrastructure Vulnerability Assessments
Abstract:	
<p>The presentation will outline the reasons for a vulnerability assessment and will also provide a live demonstration on an infrastructure vulnerability assessment. Attendees will take away the knowledge and language to articulate to senior management the organizational benefits for performing an internal vulnerability assessment. We will focus on Windows servers, UNIX (Linux) and databases (Oracle and SQL Server) and provide an efficient methodology for performing each phase of a vulnerability assessment for these systems. Participants will see tools such as Nmap, Nessus, and other Windows null session exploit tools, password cracking etc., and demonstrations on how to conduct their own assessments using these tools. Attendees will gain a heightened level of awareness of how to identify where gaps may exist in their own organization.</p>	
Target Audience:	
<p>IT Audit Managers/Directors, IT auditors, and IT security specialists that have a working knowledge of Windows/Linux, databases and networks – intermediate to advanced skill levels.</p>	
COBIT Objectives:	
Speaker Bio:	



Derek Koopowitz – CISA

IT Audit Manager at California State Automobile Association (CSAA – AAA Northern California) – based in San Francisco. Derek has been working in IT since 1978 with the last 9 years in Internal Audit – 4 years at CSAA. Prior to CSAA, he worked as an audit/security consultant at Chevron for 5 years doing audit work all over the world. Overall, he spent almost 17 years working at Chevron as a consultant in various IT capacities and prior to that spent over 5 years at Bechtel as a consultant on various software projects. Derek currently has 4 IT auditors at CSAA with openings for 2 additional auditors in our Glendale, AZ office. The majority of audits at CSAA are very technical and focus on Windows server, UNIX, Oracle, MS SQL server, and networks. We also provide ongoing consulting to our IT division which is located in Glendale, AZ along with reviewing major software/hardware projects that are in flight. Derek has a Diploma in Electronic Data Processing from Witwatersrand College for Advanced Technical Education in South Africa.

Norm Gutierrez – CISA, CISSP

Senior IT Auditor at CSAA – based in San Francisco. Norm has been in the IT Industry for 18 years. Early in his career he was a consultant and a Novell Certified Netware Engineer (CNE) focusing on clients in the investment banking arena in San Francisco. During the mid 90's, Norm worked in the Silicon Valley where he held various engineering positions working closely with high-tech giants, such as Cisco and Intel. His extensive experience with hardware certifications, standards and partnerships with Novell, Microsoft and Redhat landed him opportunities during the dot.com boom where he experienced the value and need for IT controls. During his IT Audit career with CSAA, Norm has always evangelized the need for highly technical audits to gain an effective understanding of problems that an organization may be facing. Norm has a Bachelor's degree in Computer Science from San Francisco State University.

Rob McIndoe - CISSP, GSEC, CISA, CCNA, MCSE, MCT

Senior IT Auditor at CSAA – based in Glendale, AZ. Rob has been working in Information Security since 1995, beginning his career architecting and securing classified networks for the United States Air Force. He has also been an instructor providing training for the MCSE tracks for both Windows NT and Windows 2000. Prior to CSAA, Rob worked for Charles Schwab where he performed all web application security testing for their web sites and brought his experience to provide awareness and training to the Schwab development community of the ramifications of attacks like cross-site scripting and SQL injection. While at Schwab, he played a key role in institutionalizing the Open Web Application Security Project (OWASP) web application secure coding standards now in use at Schwab. He is a member of ISACA, ISSA, IIA, and IEEE. Rob has Master's degree in Management of Information Systems Security from Colorado Technical University.

Session #T3

Presenter:	Armando Bioc
Presentation Title:	Hacking 101: Understanding the Top Web Application Vulnerabilities and How to Protect Against the Next Level of Attack.
Abstract:	
<p>The shift in focus from network-based vulnerabilities to application-based vulnerabilities has left many government organizations exposed and with the increasing threats of cyber attacks, application security has become an essential element in the application development lifecycle. Analysts have estimated that 75 percent of online attacks target web applications yet many organizations are doing very little to protect these vulnerable web applications.</p> <p>The OWASP Top Ten was created to help organizations and government agencies focus on the most serious web application security vulnerabilities. Adopting a security testing process to monitor for, identify and remediate these "Top Ten" flaws is perhaps the most effective first step towards ensuring the security of your web applications. Watchfire will provide an informative discussion and demo of the OWASP Top 10 web application attacks. This session will also provide a comprehensive overview of web application security and will highlight examples of common Web application vulnerabilities (including Cross-site Scripting, SQL Injection) and demonstrate how to defend against attacks at the Web application layer.</p> <p>This session will also discuss key principles for building security into your SDLC, techniques and best practices to proactively manage web application security and how to effectively build application security testing into the software development lifecycle (SDLC) including understanding regulatory compliance, as well as ways to safeguard the privacy and confidentiality of highly sensitive online information.</p>	
Target Audience:	
<p>Hacking 101: Skill level beginner to intermediate Occupation: IT Auditors and IT Security Professionals</p>	
COBIT Objectives:	
<ol style="list-style-type: none"> 1. Watchfire will provide an informative discussion and demo of the OWASP Top 10 web application attacks. 2. Best practices for security testing and how to effectively manage application security throughout software development lifecycle. 3. How to better understand potential web application security vulnerabilities 4. The importance of detecting and removing software vulnerabilities during application development 	
Speaker Bio:	
<p>Armando Bioc is a Security Consultant with Watchfire. Mr. Bioc provides presales technical support for AppScan sales, training for AppScan customers, security consulting within the web application software development lifecycle and web application vulnerability assessments. Mr. Bioc has been with Watchfire since 2000.</p>	

Bios



Daniel Morrison

Dan has over twenty years of industry experience designing and implementing technology and security solutions in all areas of information technology, with specialties in performance improvement, risk management, privacy, infrastructure and application security, advanced card technologies, and biometrics - within financial services, healthcare, insurance, manufacturing, and government organizations.

Dan's focus is on helping companies realize business value by leveraging technology and implementing process improvements that provide measurable results in terms of increased revenues, decreased cost, decreased time-to-market, reduced risk and improved quality.

Prior to PwC Dan worked for American Express as Chief Security Strategist where he created and led American Express Security and Privacy consulting practice. Dan also led the Security Engineering Initiative as a Senior Vice President with Bank of America, and as a Partner with Arthur Andersen, Dan was responsible for providing the global leadership and direction for Information Security Products and Services.

Dan is a Certified Information Security manager (CISM) and Certified Six Sigma Professional who has participated and managed projects throughout the United States, Canada, South Korea, Japan, South Africa and Europe.

Dan has been a speaker at many conferences and has published numerous information technology security related papers. Dan is also a member of the American Bar Association (ABA), the Information Systems Audit and Controls Association (ISACA), the Armed Forces Communications and Electronics Association (AFCEA), and the Computer Security Institute (CSI).

Presentation Overview

Vendor Security Risk Management: This session will explore methods, techniques and approaches to allow organizations to quantify and manage vendor security risk. Security risks are related to vendors need to be addressed in a number of Vendor Relationship Management Life Cycle areas. This presentation will examine security risks specific to:

- a) Planning:
 - i) Defining security requirements
- b) Contracting:
 - i) Initial Assessment
 - ii) Minimum Controls
 - iii) Metrics
- c) Vendor Management:
 - i) Problem Management
 - ii) Continuous Monitoring
 - iii) Metrics Dashboard
 - iv) Ongoing Assessments
- d) Vendor Sunsetting
 - i) Transition
 - ii) Information and Asset Recovery
 - iii) Post Contract Controls

Successful Strategies for Sustained Career Growth and Marketability

The SF ISACA Fall Conference presents an outstanding opportunity to further one's knowledge of tools, techniques, and best practices to enable one to excel as an IS Auditor and advance in one's career. But this knowledge is of limited benefit if one doesn't also focus on the tools and knowledge to enable one to navigate his/her career successfully. This luncheon presentation is designed to focus on the other (non-technical) skill-sets and knowledge that are also critical to career success.

Over the past several years, audit professionals have benefited from a favorable job market unlike any we have seen before. A Sarbanes-Oxley-driven shortage of resources has created bountiful opportunities for those contemplating a career move, and it has also contributed to salary escalation. While these conditions have been a blessing for IS Auditors, they can also easily lead to choices that may negatively impact career development in the long-term. Moreover, in this day and age of corporate downsizing, rightsizing and outsourcing, it still remains a great challenge to navigate one's career successfully. In this environment of ubiquitous opportunity, it is perhaps even more important to make sound career decisions.

In this presentation, we will focus our attention on the many challenges of successfully managing one's career. We will also address strategies and techniques to help maintain one's marketability while avoiding costly career mistakes. Some of the topics to be covered include:

- Key success factors for sustained career growth
- Evaluating your skills by focusing on Core Competencies
- Taking an organic approach to career development
- The challenge of balancing life and career goals
- Strategies for approaching both good and bad job markets
- Tips for positive career growth
- Avoiding costly career mistakes

Todd Weinman is Lander International's Regional Recruiting Director for the Western United States. Todd is a graduate of UC Berkeley and worked for several years for a local Big 5 public accounting firm prior to entering the field of Executive Recruiting. As a recruiter, Todd enjoys visiting audit, information security, and consulting departments throughout the Western United States, and he is in contact on a daily basis with scores of Directors, Managers and staff level professionals from around the region. Todd has become a frequent speaker for ISACA and IIA, to local universities, to the Group of 25, and to audit committees. He has been on the Board of Directors for the San Francisco chapter of ISACA since 1998 and has served a term as chapter President. Todd has also written or been interviewed for numerous publications and professional journals, including the Wall Street Journal.

Todd strives to extend the role of executive recruiter to be a true career counselor, and he has authored numerous articles for professional journals. In June of 1999 Todd was honored by the California Association of Personnel Consultants at its annual conference by receiving the coveted “Consultant of the Year” award. One individual recruiter in the entire state was singled out for this honor.

Todd is an advocate of living the well-balanced life. When he is not recruiting, Todd pursues his passion for music as a professional classical musician. In addition to having spent four years performing with the Philharmonic Orchestra of Santiago, Chile, Todd has performed music on four continents, and he has performed with a variety of Northern California ensembles, including the San Francisco Symphony, Stockton Symphony, and Yo-Yo Ma's Silk Road Ensemble, and the Aspen Summer Music Festival.