



ISACA's 2012 North America CACCS Conference

7-10 May 2012 | Loews Royal Pacific Resort at Universal Orlando® | Orlando, Florida, USA



What's Next Starts Here ...

North America Computer Audit, Control and Security Conference

- Over 70 thought-provoking sessions focusing on today's top assurance, risk and security topics
- Seven pre and post conference workshops covering emerging trends, best practices and biggest challenges facing IT audit and security professionals
- Over 100 industry renowned speakers
- A unique educational experience offering up to 44 CPE hours

Why Wait?

Register by 16 March 2012 and save US \$200



Follow us on Twitter @ISACANews and use the hash tag #NACACS

ISACA[®]
Trust in, and value from, information systems

About the Conference

North America CACS, ISACA's legacy conference, is truly where eager minds come together to connect and learn. The content-rich sessions delve into some of the biggest challenges facing today's information technology professionals.

2012 Solution Center. Tour the floor and gain insight into emerging products and solutions while networking with the biggest players from across the industry.

Expand Your Connections. We understand that North America CACS is not just about education, it's about networking too. That is why we incorporated more than **8 hours** of network time with your peers and solutions experts.

Get the Most from Your Experience. Our 2012 agenda includes **100+ speakers in 70+ sessions**, with loads of content available for industry newcomers right through to advanced C-level executives.



North America CACS 2012 Conference Task Force

Charlie Blanchard, CISA, CISM, CRISC (Chair)
Manager, Security and Privacy Services
Deloitte & Touche LLP

David Baker, CISA
Sr. Manager, Professional Practices
Sara Lee

Mario D'Alicandro, CISA
Director
Protiviti

James T. Enstrom, CISA, CRISC
Director, Information Technology Audit
Chicago Board Options Exchange

Jill Farrington
Partner
KPMG LLP

Scott M. Shinnars, CISA
Finance Director
ConAgra Foods Inc.

Mary Ann Stoltenberg-Smith, CISA, CISM, CRISC
Vice President & IT Audit Manager
Federal Reserve Bank of Chicago

Michael Walsh, CISA, CISM, CRISC
Info Sec Consultant
IKE Consulting LLC

Keynote Speakers



Trends and Technology—Taking the Lead

Scott Klososky

Founder and Board Chair

Alkami Technology

www.klososky.com

Scott is the founder of Alkami Technology where he currently serves as board chair. Alkami has developed a second generation online banking platform that provides many new features that do not exist today in current online banking systems. In the past, he served as an aide to President Nixon and worked as a turnaround CEO for Critical Technologies where he completely rebuilt the company, restoring its status to profitability. Scott also founded Webcasts.com and Paragraph, Inc. His vision and ability to see trends in emerging technologies allows him to be a thought leader who applies his skills to help organizations thrive, leaders prosper, and entire industries move forward.

This innovative keynote provides a top-to-bottom tutorial on the best practices for implementing a social technology (social media, social networking and social relevance) strategy with impact. It is important to note that this is not a session that teaches best practices for using LinkedIn or Facebook. This is a robust keynote backed by strong explanations of why social technology matters, and how it is changing sales process, customer service and marketing. Technology tools and trends powerfully impact how organizations communicate and stay relevant. Areas specifically covered include: online reputation management, crowdsourcing, building rivers of knowledge, and becoming industry experts. Even the smallest improvements in leveraging social technology can propel your organization to leapfrog your competitors.



Become a Change Agent—Bringing What You Gained at the Conference Into Your Organization

Ed Robinson, CPA, CSP

President and CEO

Robinson Performance Group

www.edspeaks.com

A certified speaking professional, Ed is the author of four books and recognized expert in practice and business growth. His energetic, engaging and entertaining style is a primary reason why Ed's strategies improve performance. As a result, he helps individuals manage change and increase revenue regardless of economic obstacles and challenges. A self-described "recovering CPA", Ed is bringing his vast experience, proven leadership and practiced motivational style to NACACS 2012. With over 30 years experience in professional service organizations, Ed provides growth strategies that are unique, even amongst the leadership consulting landscape. Having spoken in over 25 countries, Ed is sought after globally for his speaking style and coaching techniques.

We are all being challenged by new ways of doing business. These challenges can include industry or regulatory changes as well as colleagues who just do not see the need to change. In this closing session, you will gain core, universal strategies to flourish and thrive in the ever-changing, constantly shifting information technology industry. Ed will help you retain and implement what you learn at NACACS 2012. Leave with a renewed commitment to professionalism and productivity as you gain formulas for success and learn the key attributes of professionalism, personal success and self-motivation.

Conference at a Glance

Pre-conference Workshops

Saturday 5 May 2012

9:00 AM–5:00 PM	WS1	Control and Security of Web Applications	Kevin Nibler, <i>Canaudit Inc.</i>
	WS2	IT Risk Management	Shawna M. Flanders, CISA, CISM, CRISC, <i>PSCU Financial Services</i>
	WS4	Performing IT Audits: A Practical Approach	Phil Flora, CISA, <i>FloBiz & Associates, LLC</i>

Sunday 6 May 2012

9:00 AM–5:00 PM	WS1	Control and Security of Web Applications (cont.)	Kevin Nibler, <i>Canaudit Inc.</i>
	WS2	IT Risk Management (cont.)	Shawna M. Flanders, CISA, CISM, CRISC, <i>PSCU Financial Services</i>
	WS5	Server Virtualization Security and Audit	Michael T. Hoelsing, CISA, <i>University of Nebraska at Omaha</i>

5:30–7:30 PM **Welcome Reception** Join us for the opening event of North America CACS. A highly interactive environment in an informal setting, this is an ideal time to begin networking with your peers and engage with many of the speakers. Do not miss this opportunity to reunite with friends and colleagues from around the world and meet seasoned professionals as well as newcomers.

Monday 7 May 2012

8:30–9:55 AM	OPENING KEYNOTE: Trends and Technology Scott Klososky, Founder and Board Chair, <i>Alkami Technology</i>		
10:15–11:45 AM	T1	111 Business Impact of IT Audit Issues	Jeff Roth, CISA, CGEIT, <i>Parsons</i>
	T2	112 What is Virtualization and How Do I Audit It?	Rick Schnierer, CISA, CRISC, <i>Nationwide Insurance</i> ; Chris Tennant, CISA, CRISC, <i>Nationwide Insurance</i>
	T3	113 Automating IT Data Collection and Compliance for GRC Controls	Jason Creech, <i>Qualys</i>
	T4	114 Emerging IT Risks Panel Discussion	Jill Farrington, <i>KPMG LLP</i> ; David Baker, CISA, <i>Sara Lee</i> ; Scott M. Shinnars, CISA, <i>ConAgra Foods Inc.</i>
	T5	115 IT Governance Considerations with Mobile Computing	Phil Lageschulte, CGEIT, <i>KPMG</i> ; Martin Sokalski, <i>KPMG LLP</i>
	T6	116 New for 2012: Emerging IT Audit Risks	Michael Juergens, CISA, CGEIT, CRISC, <i>Deloitte</i>
	T7	117 Enterprise Risk Management Essentials	James Ambrosini, CISA, CRISC, <i>Protiviti</i>
1:30–3:00 PM	T1	121 Developing a Risk-based Audit Plan	Phil Flora, CISA, <i>FloBiz & Associates, LLC</i>
	T2	122 The Keys to Assessing Risk when Sharing Data with Service Providers	Dave Kovarik, CISM, <i>Northwestern University</i>
	T3	123 Does Your Organization Need a Risk Management Plan for Personally Identifiable Information Data?	Jeff Kalwerisky, <i>CPEInteractive Inc.</i>
	T4	124 Emerging IT Risks Roundtable	Jill Farrington, <i>KPMG LLP</i> ; Mary Ann Stoltenberg-Smith, CISA, CISM, CRISC, <i>Federal Reserve Bank of Chicago</i> ; David Baker, CISA, <i>Sara Lee</i> ; Scott M. Shinnars, CISA, <i>ConAgra Foods Inc.</i>
	T5	125 Regulator Hot Topic Panel Visit www.isaca.org/2012nacacs for up to the minute conference information and session announcements.	Panel of Industry Experts
	T6	126 System Authentication: The New Risk and 7 Steps to Audit and Remediate	Jeff Hudson, <i>Venafi</i>
	T7	127 IT Risk Management Life-cycle and Enabling IT with GRC Technology	Debbie Lew, CISA, CRISC, <i>Ernst & Young LLP</i> ; Steven F. Jones, <i>Ernst & Young LLP</i>
3:30–5:00 PM	T1	121 Developing a Risk-based Audit Plan (cont.)	Phil Flora, CISA, <i>FloBiz & Associates, LLC</i>
	T2	132 Auditing Mobile Computing/Consumerization of IT	Deron Grzetich, CISM, <i>KPMG LLP</i>
	T3	123 Does Your Organization Need a Risk Management Plan for Personally Identifiable Information Data? (cont.)	Jeff Kalwerisky, <i>CPEInteractive Inc.</i>
	T4	134 A Lesson for Leaders: How to Attract and Retain Top Personnel in Today's Economy	Derek Duval, <i>Duval Search Associates</i>
	T5	135 Trends in Compliance and Regulations	Panel of Industry Experts
	T6	136 Auditing Cloud Computing and Outsourced Operations	Mike Schiller, CISA, <i>Texas Instruments</i>
	T7	137 Reduce IT Risk Through Improved Management and Planning	Gary Alterson, CISA, CRISC <i>Neohapsis</i>

All sessions are recommended for professionals with 3 or more years of IT experience and a working knowledge of IT terminology.

Tuesday 8 May 2012

8:30–10:00 AM	T1	211	Data Analytics for IT Governance Controls	Michael T. Hoelsing, CISA, <i>University of Nebraska at Omaha</i>
	T2	212	Auditing Your Unix and Linux Operating Systems	Mike Schiller, CISA, <i>Texas Instruments</i>
	T3	213	Records and Information Management: Understanding the Risks and Operational Challenges	David Melnick, CISA, <i>Deloitte</i>
	T4	214	Changing the C-Suite Perception of Internal Audit	Princy Jain, CRISC, <i>PricewaterhouseCoopers</i> ; Linda Glaub, <i>Citrix Systems, Inc.</i> ; Scott Moreland, CISA, CRISC, <i>Raymond James Financial</i> ; Abhijit Pandit, CISA, <i>Adobe Systems, Inc.</i> ; Dan Williams, <i>Darden</i>
	T5	215	Implementing COBIT Quickstart in a Healthcare Organization	Nelson Gibbs, CISA, CISM, CGEIT, CRISC
	T6	216	In the Crosshairs of Social Engineering Attacks	Eric Olson, <i>Cyveillance, Inc.</i>
	T7	217	The Opportunity in Risk and Security Trends	Tom Patterson, CISA, CGEIT, CRISC, <i>IBM Global Services</i>
10:30 AM–12 NOON	T1	221	Networking and Building Relationships	Debbie Lew, CISA, CRISC, <i>Ernst & Young LLP</i>
	T2	222	Microsoft SQL Database Auditing	Don Campanaro, CRISC, <i>National Grid</i> ; Janet Petrofere, CISA, CRISC, <i>National Grid</i>
	T3	223	Recent Legal and Technical Trends in Privacy and Data Protection	Wayne C. Matus, <i>Pillsbury Winthrop Shaw Pittman</i> ; Kenneth B. Leissler, <i>Protiviti Inc.</i>
	T4	224	Healthcare Security: Learning from Rigorous Government Security Requirements	Todd Fitzgerald, CISA, CISM, CGEIT, CRISC, <i>ManpowerGroup</i>
	T5	225	Data Quality and Data Classification—Comparisons, Efficiencies and Success Factors	Gary Alterson, CISA, CRISC, <i>Neohapsis</i>
	T6	226	Secure Coding: Best Practices	Industry Expert
	T7	227	What Color is Your Information Risk—Today?	Jim Hurley, <i>Symantec Corporation</i>
1:30–3:00 PM	T1	231	Auditors Guide to Process Improvement, Innovation and Business Process Management	Shawna M. Flanders, CISA, CISM, CRISC, <i>PSCU-FS</i>
	T2	232	Auditing Oracle ERP	Reshad Alam, <i>Regal Beloit</i> ; Tim Van Ryzin, CISA, CISM, <i>Regal Beloit</i>
	T3	233	Using Encryption Technologies to Protect Data	Alfred John Bacon, CISA, CISM, <i>PETROBRAS</i>
	T4	234	Mobile Device Security, Privacy, and Data Protection	Michael Davis, <i>Savid Technologies, Inc.</i>
	T5	235	eDiscovery: Trends, Leading Practices, Risks, and Controls	Scott M. Shinnors, CISA, <i>ConAgra Foods, Inc.</i>
	T6	236	Reduce Cloud Security and Compliance Risks by Automating Privileged Accounts	Adam Bosnian, <i>Cyber-Ark Software</i>
	T7	237	Security Auditing and Governance for Healthcare Providers	Tom Turo, CISM, CRISC, <i>Adventist Health System</i> ; Sharon Finney, CISM, <i>Adventist Health System</i> ; Steve Stallard, <i>Orlando Health</i> ; Christi Rushnell, <i>Health First</i>
3:30–5:00 PM	T1	241	Embedding Data Analytics in Your Process and Continuous Fraud Auditing	Brooke Miller, <i>RLI Insurance Company</i> ; Sean Scranton, CISA, CISM, CRISC, <i>RLI Corp</i>
	T2	242	Networking and Telephony	Scott M. Baron, CISA, CRISC, <i>National Grid</i>
	T3	243	Data Breach and Trade Secret Theft: How a Holistic Approach Can Protect Your Assets	William Hardin, <i>Navigant</i> ; Brad Pinne, <i>Navigant</i>
	T4	244	SAP: Real Time Controls in the SAP Environment	Steve Oberhauser, CISA, <i>KPMG</i>
	T5	245	Healthcare Privacy and Security Landscape in 2012	Todd Fitzgerald CISA, CISM, CGEIT, CRISC, <i>ManpowerGroup</i> ; Cliff Baker, <i>HITRUST Alliance</i>
	T6	246	Social Media Risk and Mitigation Guidance	Rumy Jaleel-Khan, CISA, CRISC, <i>Deloitte</i> ; Mike Wyatt, CISA, <i>Deloitte & Touche LLP</i>
	T7	247	Black Holeistic Disaster Recovery: How to Limit Losses	Donald Gallien CISA, CISM, <i>American Express</i> ; Dave Mabery, <i>American Fidelity Assurance Company</i>
5:00–6:30 PM	Solution Center Reception Marking the official opening of the <i>InfoExchange!</i> Collaborate with peers, interact with thought leaders and get a glimpse into the hottest emerging solutions available for IT professionals. Join us for this valuable event!			

Wednesday 9 May 2012

8:30–10:00 AM	T1	311	Career Development for IT Auditors	Derek Duval, <i>Duval Search Associates</i>
	T2	312	The Risk and Exposure of Today's Top Web Application Security Risks (OWASP Top 10)	Kevin Nibler, <i>Canaudit Inc.</i>
	T3	313	Developing and Deploying an Enterprise Strategy for Information Loss Prevention	Kevin Novak, CISM, <i>Northern Trust</i>
	T4	314	NEW TOPIC! Data Security & Privacy: Can it Be Institutionalized?	Sophia Schell, CRISC, <i>IBM</i>
	T5	315	Certificates—The New Authentication: Risks and Remediation	Paul Turner, <i>Venafi</i>
	T6	316	Identify and Eradicate: The Top Security Threats to Banks in 2012	Russ Horn, CISA, CRISC, <i>CoNetrix</i>
	T7	317	Establish and Maintain Information Security Oversight	Daniel Dec, CISA, CISM, <i>Cognizant Technology Solutions</i>

Wednesday 9 May 2012 (cont.)

10:00AM-1:30PM	Solution Center			
1:30-3:00PM	T1	321	An Integrated Approach to Process-based IT Audit Using Quality and Information Security Management Systems	Ashit Dalal, CISA, CISM, CGEIT, CRISC, <i>eDelta Consulting</i>
	T2	322	SAP: Segregation of Duties for SAP and Oracle	Alfred John Bacon, CISA, CISM, CRISC, <i>PETROBRAS</i>
	T3	323	Understanding and Mitigating System, Compliance and Legal Consequences of Cloud Computing	Michelle V. Crawford, CISA, <i>Alabama State University</i>
	T4	324	Is IT Still Relevant? Communicating Trends and Risks Found in the New Technology Landscape	Robert E. Stroud, CGEIT, CRISC, <i>CA Technologies</i>
	T5	325	Beyond Compliance: Reduce Operation Risk and Cost While Complying	Sven Skoog, CRISC, <i>IBM</i>
	T6	326	After the Breach	Ray Soriano, CISA, CISM, CRISC, <i>Deloitte & Touche LLP</i>
	T7	327	SaaS: How to Secure the Services Your Team Provides	Michael Davis, <i>Savid Technologies, Inc.</i>
3:30-5:00 PM	T1	331	Design and Deliver Report Presentations that Speak to Your Target Audience and Drive Action	Janelle Brittain, <i>Dynamic Performance Institute, LLC</i>
	T2	332	ITIL and CMM Assessments for IT Operations	Sameer Gupta, <i>KPMG LLP</i>
	T3	333	Reform Of The European Union Data Protection Framework— A US Perspective	Charlie Blanchard, CISA, CISM, CRISC, <i>Deloitte</i>
	T4	334	Incident Management	Jeff Roth, CISA, CGEIT, <i>Parsons</i>
	T5	335	Review FFIEC Supplemental Guidance on Internet Banking Authentication, Combat Internet Banking Risks	Russ Horn, CISA, CRISC, <i>CoNetrix</i>
	T6	336	How to Conquer the Social Media Landscape: The Vanguard Experience	Theodore H. Wolff, CISA, <i>Vanguard</i>
	T7	337	CFO and CIO: Partners or Opponents?	Daniel Dec, CISA, CISM, <i>Cognizant Technology Solutions</i>
6:00-8:00 PM	Networking Reception			

Thursday 10 May 2012

8:30-9:45 AM	T1	411	Migrating to COBIT 5 for Auditors	Anthony Noble, CISA, <i>Viacom</i> ; Rob Johnson, <i>Bank of America</i>
	T2	412	Tips, Techniques, and Tools for Completing a PCI Self Assessment Questionnaire (SAQ)	William L Wayland, CISA, <i>Experis (Formerly Jefferson Wells)</i>
	T3	413	A New Opportunity for IT Professionals: PS-Prep™ Audit	Lynnda M. Nelson, <i>ICOR</i> ; Paul Burck, <i>Oriion</i> ; Kathy Glynn, <i>GAP Resources</i> ; Scott Richter, <i>ANSI-ASQ National Accreditation Board</i> ; James Nelson, <i>Business Continuity Services, Inc.</i> ; Marcus Pollock, <i>FEMA/DHS</i> ; Timothy Woodcome, <i>NQA-USA</i>
	T4	414	Understanding Your Data Flow: Using Tokenization to Secure Data	Ulf Mattsson, <i>Protegrity</i>
	T5	415	IT Governance: Myth to Reality	Michael Bargerhuff, CRISC, <i>Ultimate Software</i>
	T6	416	Protecting Your Mobile Devices	Nelson Gibbs, CISA, CISM, CGEIT, CRISC
	T7	417	How to Make Enterprise Governance, Risk and Compliance (eGRC) Work for You	Kevin Novak, CISM, <i>Northern Trust</i>
10:00-11:15 AM	T1	421	Auditing the Intangible: Tangible Techniques for Assessing the Internal Control Environment	Industry Expert
	T2	412	Tips, Techniques, and Tools for Completing a PCI Self Assessment Questionnaire (SAQ) (cont.)	William L Wayland, CISA, <i>Experis (Formerly Jefferson Wells)</i>
	T3	413	A New Opportunity for IT Professionals: PS-Prep™ Audit (cont.)	Lynnda M. Nelson, <i>ICOR</i> ; Paul Burck, <i>Oriion</i> ; Kathy Glynn, <i>GAP Resources</i> ; Scott Richter, <i>ANSI-ASQ National Accreditation Board</i> ; James Nelson, <i>Business Continuity Services, Inc.</i> ; Marcus Pollock, <i>FEMA/DHS</i> ; Timothy Woodcome, <i>NQA-USA</i>
	T4	424	How to Protect Your Network when Social Media Drives Malware Delivery Vehicle	Paul Henry, <i>Lumension</i>
	T5	425	Information Warfare: Because Weapons Aren't Always Made of Steel	Brian Contos, <i>McAfee</i>
	T6	426	Wikileaks: Are You the Next Target?	Richard Payne, CISM, CGEIT, CRISC, <i>IBM Business Consulting Service</i>
	T7	417	How to Make Enterprise Governance, Risk and Compliance (eGRC) Work for You (cont.)	Kevin Novak, CISM, <i>Northern Trust</i>
11:30 AM-12:30 PM	CLOSING KEYNOTE: Become a Change Agent—Bringing What You Gained at the Conference Into Your Organization			Ed Robinson, CPA, CSP, President and CEO, <i>Robinson Performance Group</i>
1:30-5:00 PM	WS6	Cloud Computing Audit and Assurance Issues		Dan Cimpean, CISA, CGEIT, <i>Deloitte</i> ; Cedric Lempereur, CISA, CISM, <i>Deloitte</i>
	WS7	Data Loss Prevention (DLP)		Kyle Harvey, CISA, <i>Ernst & Young LLP</i> ; Chip Wentz, CISA, CISM, CGEIT, <i>Ernst & Young LLP</i>
Friday 11 May 2012				
8:30 AM-12 NOON	WS6	Cloud Computing Audit and Assurance Issues (cont.)		Dan Cimpean, CISA, CGEIT, <i>Deloitte</i> ; Cedric Lempereur, CISA, CISM, <i>Deloitte</i>
	WS7	Data Loss Prevention (DLP) (cont.)		Kyle Harvey, CISA, <i>Ernst & Young LLP</i> ; Chip Wentz, CISA, CISM, CGEIT, <i>Ernst & Young LLP</i>

Post-conference Workshops

NACACS 2012 Session Descriptions

All sessions are recommended for professionals with 3 or more years of IT experience and a working knowledge of IT terminology.

Track 1 Accelerating IT Audit Concepts

Technical and legislative environments require IT audit professionals to know the key to good practice auditing, from how to set up a risk-based audit plan to performing value-added audits, using state of the art tools and methods. This track presents topics essential to IT audit professionals to perform their jobs competently. The sessions are designed to provide concepts, methodologies and techniques to help the participants improve upon their knowledge, expertise and skills.

111

Business Impact of IT Audit Issues

Jeff Roth, CISA, CGEIT
Information Systems Assurance Engineer
Parsons

After completing this session, you will be able to:

- Recognize that greater business knowledge increases the relevance of IT audit results and recommendations.
- Identify the business impact and quantify the risk of audit findings
- Discuss issues with key stakeholders with great ease and in terms they are able to appreciate and address

121

Developing a Risk-based Audit Plan

Phil Flora, CISA
Principal
FloBiz & Associates, LLC

After completing this session, you will be able to:

- Identify standards related to risk assessment and audit planning
- Provide risk management framework examples for application/use in identifying organizational risks
- Determine ways that COBIT and Risk IT can be used to facilitate the risk assessment process
- Identify challenges & opportunities in the information gathering process
- Provide risk assessment/audit planning process/steps for the total audit universe
- Determine methods/approaches to communicate audit planning process results for review/approval

211

Data Analytics for IT Governance Controls

Michael T. Hoelsing, CISA
Faculty
University of Nebraska at Omaha

After completing this session, you will be able to:

- Identify topical areas in a mainframe environment that are candidates for data analysis (change management, logical access, configuration management, job scheduling, and more)
- Identify data sources needed to perform analysis of the above areas
- Develop analysis techniques using typical audit department tools
- Report exceptions to assist with control remediation

221

Networking and Building Relationships

Debbie Lew, CISA, CRISC
Senior Manager
Ernst & Young, LLP

After completing this session, you will be able to:

- Gain an understanding of the benefits and basics of effective networking including the fine art of small talk
- Keep track and expand pool of contacts
- Develop both an internal and external network
- Follow up and Follow through after making contact to produce meaningful results and build relationships
- Learn other ways to network other than meeting in social situations

231

Auditors Guide to Process Improvement, Innovation and Business Process Management

Shawna M. Flanders, CISA, CISM, CRISC
Productivity Specialist
PSCU-FS

After completing this session, you will be able to:

- Differentiate between Project Management, Auditing, Process Improvement and Process Innovation, and understand the benefit to the organization
- Identify where and how a Risk Management Framework can be applied in an organization
- Recognize the risks and rewards, and tools of Business Process Management
- Conduct an audit for reviewing processes or applications with Process Improvement and/or BPM (or CRM) components.
- Conduct an audit on a BPM application.
- Conduct an audit on a Process Improvement Project



NACACS 2011 Deloitte prize drawing



Orlando

241

Embedding Data Analytics in Your Process and Continuous Fraud Auditing

Brooke Miller
Audit Manager
RLI Insurance Company

Sean Scranton, CISA, CISM, CRISC
Director, IT Audit
RLI Corp

After completing this session, you will be able to:

- Understand how to embed data analytics in the audit process
- Transition to a continuous auditing approach
- Identify and prevent fraud and funds leakage
- Use red-flag indicators to reduce false positives, be risk focused, and save time in continuous auditing

311

Career Development for IT Auditors

Derek Duval
Owner
Duval Search Associates

After completing this session, you will be able to:

- Identify key technical skills requirements
- Learn how to garner needed business knowledge
- Identify the 10 habits of highly successful audit professionals
- Brand truth and myths
- Conceptualize career advancement
- Gain a perspective of some future challenges you will face

321

An Integrated Approach to Process-based IT Audit Using Quality and Information Security Management Systems

Ashit Dahal, CISA, CISM, CGEIT, CRISC
Managing Consultant and Sr. Manager
eDelta Consulting

After completing this session, you will be able to:

- Discover key requirements of Integrated Management Systems as applied to enterprise IT environment
- Define, assess and evaluate the process-based audit approach implementing conventional checklist-based audit methodology
- Adopt and deploy integrated and process-based IT audit approach to conduct value-based audit of the organization's IT and IS systems
- Plan and implement effective process-based audit approach using "PEAR" tool
- Demonstrate compliance with applicable requirements like SAS-70, PCI-DSS, COBIT

331

Design and Deliver Report Presentations that Speak to Your Target Audience and Drive Action

Janelle Brittain
CEO
Dynamic Performance Institute, LLC

After completing this session, you will be able to:

- Design the report presentation to meet the goals for that audience
- "Speak the Language" of the report listeners to increase their understanding and acceptance
- Keep yourself in control when others are defensive
- Positively handle delivering the "Bad News"
- Handle the Q&A with finesse

411

Migrating to COBIT 5 for Auditors

Anthony Noble, CISA
VP IT Audit
Viacom

Rob Johnson, CISA, CISM, CGEIT, CRISC
SVP GTO-Audit/IT Risk
Bank of America

After completing this session, you will be able to:

- Understand the COBIT 5 content equivalent from COBIT 4.1
- Recognize how the new content/guidance of COBIT 5 enhances the auditor's effort
- Realize how auditors can use this revised and new content in their audit work

421

Auditing the Intangible: Tangible Techniques for Assessing the Internal Control Environment

Industry Expert

After completing this session, you will be able to:

- Explore the challenges faced in assessing an internal control environment.
- Learn practical techniques for obtaining indirect evidence through periodic audits
- Assess the strength of the control environment by drawing inferences about "soft" controls from "hard" evidence
- Present a compelling audit proposition by interconnecting risks faced across entity, process and system levels

Track 2 Tools and Techniques for IT Audit Programs

The IT audit and assurance professional must have a clear understanding of the underlying business processes and techniques to assess the adequacy of controls within these processes. Through demonstration and discussion of audit programs, this track will help IT audit professionals identify technological risks to the business and operational environments and how to use relevant business analysis as well as IT audit tools and techniques. These hands-on sessions are presented at an intermediate to advanced level. Each session combines process analysis and audit methodology with practical knowledge and examples to clearly illustrate best practices needed by today's IT audit and assurance professionals.

112

What is Virtualization and How Do I Audit It?

Rick Schnierer, CISA, CRISC

*Associate Vice President, Internal Audit
Nationwide Insurance*

Chris Tennant, CISA, CRISC

*Audit Consultant, Internal Audit
Nationwide Insurance*

After completing this session, you will be able to:

- Understand the fundamentals of virtualization and supporting architecture
- Develop and execute a risk based audit for VMware ESX servers
- Identify best practices for securing VMware ESX servers, access to the management console, and other key configurations related to virtual servers
- Leverage the lessons learned from our review and apply this to your environment

122

The Keys to Assessing Risk when Sharing Data with Service Providers

Dave Kovarik, CISM

*Director, Information & Systems Security/Compliance
Northwestern University, Information Technology*

After completing this session, you will be able to:

- Recognize the process established to assess the control environment of the service provider
- Understand the risk inherent with sharing data with a 3rd party
- Help convey the risk to the client
- Assist the client in making an informed decision in the selection of a vendor

132

Auditing Mobile Computing/ Consumerization of IT

Deron Grzetich, CISM

*Manager
KPMG LLP*

- Understand why utilizing the most current software and applications is critical and how to test them

- Develop a policy to ensure compliance and a process to protect against violations
- Create a recovery policy for protecting the mobile user and information stored on mobile devices

212

Auditing Your Unix and Linux Operating Systems

Mike Schiller, CISA

*Director of Global Server, Database, and Storage Infrastructure
Texas Instruments*

After completing this session, you will be able to:

- Perform audits on Unix and Linux systems, focusing on the following areas:
 - Account management and password controls
 - File security and controls
 - Network security and controls
 - Audit logs
 - Security monitoring and general controls
- Access tools and resources for performing Unix and Linux audits.

222

Microsoft SQL Database Auditing

Don Campanaro, CRISC

*Sr. Auditor
National Grid*

Janet Pietroferre, CISA, CRISC

*Global Digital Risk & Security Compliance Manager
National Grid*

- Learn how to adapt the user and schema design to maximize SQL server reliability and to ensure that your enterprise is able to maximize delivered analytics
- Identify the audit and security review objectives right for your enterprise
- Discover what audit services are required to determine underlying design and implementation to ensure reliability



Everglades

232

Auditing Oracle ERP

Reshad Alam
IT Audit Manager
Regal Beloit

Tim Van Ryzin, CISA, CISM
Director, Security & IT Risk Management
Regal Beloit

After completing this session, you will be able to:

- Understand the Oracle ERP environment
- Recognize the key risks in Oracle ERP
- Learn the Oracle ERP layers and controls
- Identify business processes and controls
- Become familiar with controls consideration for existing and new ERP environment
- Leverage tools to manage audit and compliance for Oracle ERP



Citywalk

242

Networking and Telephony

Scott M. Baron, CISA, CRISC
Director, Digital Risk and Security, Governance
National Grid

- Learn how to classify a boundary between data and voice networks
- Recognize vulnerable areas, the risks they pose to the business activity and how to mitigate them
- Determine how to analyze your enterprise's telephony traffic
- Identify necessary configuration monitoring to ensure data is not compromised

312

The Risk and Exposure of Today's Top Web Application Security Risks (OWASP Top 10)

Kevin Nibler
Senior Manager, Security and Audit Services
Canaudit Inc.

After completing this session, you will be able to:

- Understand how web applications are being leveraged by malicious individuals
- Implement controls to minimize organizational risk
- Recognize proper mitigation and risk control tables
- Become familiar with and utilize OWASP's list of the Top 10 Most Critical Web Application Security Risks

322

SAP: Segregation of Duties for SAP and Oracle

Alfred John Bacon, CISA, CISM, CRISC
Senior Consultant, Internal Controls
PETROBRAS

After completing this session you will be able to:

- Grasp the importance of Segregation of Duties in the business scenario
- Understand the main issues involved in SOD analysis and why a structured database solution is necessary in large ERP environments
- Plan an SOD project, with a clear view of the main stumbling blocks
- Have a clear view of the need for business user involvement in the cleaning-up stage and in defining compensating controls
- Know what is missing in the business objects GRC Access Control reports
- Understand the difficulties in defining and documenting compensating or mitigating controls
- Present a business case for implementing an SOD tool

332

ITIL and CMM Assessments for IT Operations

Sameer Gupta
Director
KPMG LLP

After completing this session, you will be able to:

- Understand the purpose of an IT Maturity Model and where can it be leveraged
- Understand the differences in ITIL and CMMI models
- Learn about a model that covers aspects of both ITIL and CMMI
- Take a deeper dive into assessing one of the capabilities of this model
- Review reports that be generated from such an assessment

412

Tips, Techniques and Tools for Completing a PCI Self Assessment Questionnaire (SAQ)

William L Wayland, CISA
Risk Advisory Services
Experis (Formerly Jefferson Wells)

After completing this session, you will be able to:

- Identify a process enabling a company with limited resources to plan and execute an initiative to verify, and if necessary, remediate compliance with PCI-DSS requirements
- Utilize a customized Excel workbook designed with specific requirements for tracking and subsequent consolidation into the SAQ
- Understand how to integrate other regulations (ex. Massachusetts Privacy Law 201 CMR 17.00) to check for compliance
- Discuss other approaches to working with Acquirers and the Payment Brands

Track 3 Make Your Data Secure

Privacy is a growing concern as limitations seem to collapse when collecting, storing and managing data. This track will explore how the threats to privacy are evolving, how privacy can be protected and how to balance the need to collect and secure information in a fast-paced environment where electronic information is exchanged. Participants will delve into today's largest privacy threats and how IT professionals can maintain IT related risk at an acceptable level. Sessions will also cover the growing concerns over wireless/mobile communication, financial privacy, medical record confidentiality, background checks and other sources of searchable internet data.

113

Automating IT Data Collection and Compliance for GRC Controls

Jason Creech

*Director, Policy Compliance
Qualys*

After completing this session, you will be able to:

- Integrate IT asset discovery mechanisms to dynamically update the IT asset repository
- Establish detailed configuration controls and policy mappings
- Deploy automated general computer control (GCC) collection
- Avoid configuration control self-assessment and measurement
- Leverage complementary solutions to maximize your IT GRCM investment

123

Does Your Organization Need a Risk Management Plan for Personally Identifiable Information Data?

Jeff Kalwerisky

*Senior Director, Information Security & Technical Training
CPEInteractive, Inc.*

After completing this session, you will be able to:

- Understand scope and definition for the concept of Personally Identifiable Information (PII)
- Understand some of the major business risks associated with storing and processing PII
- Understand the compliance issues associated with PII in North America, Europe, Asia and the Pacific Rim
- Discuss the data privacy issues associated with use of mobile devices with geolocation capabilities

- Understand policies, roles and responsibilities required for adequate protection of PII, using the Massachusetts and California Data Breach laws as examples
- Understand the risks involved with third parties such as contractors, customers, and vendors
- Determining whether your corporation has PII, where it is located, and whether it is needed
- Develop an action plan for compliance and build a PII compliance framework
- Identify where to focus on an evaluation of PII risk and integrate PII compliance into the entity-wide compliance program

213

Records and Information Management: Understanding the Risks and Operational Challenges

David Melnick, CISA

*Principal, National Privacy and Data Protection Practice
Deloitte*

After completing this session participants will be able to:

- Demonstrate understanding of evolution of records and information life cycle management programs including overview knowledge of key drivers around regulatory compliance, eDiscovery, records retention, and operational document management.
- Recognize specific risks and the regulatory landscape and related implications around information management
- Analyze how to develop an enterprise integrated strategy around information management and to understand the security and privacy implications to the program
- Engage in a case-study based discussion of implementing an Enterprise Approach to Integrated Information Management



Citywalk

223

Recent Legal and Technical Trends in Privacy and Data Protection

Kenneth B. Leissler

Managing Director
Protiviti Inc.

Wayne C. Matus

Partner, Leader of the Information Law & Electronic Discovery Practice
Pillsbury Winthrop Shaw Pittman

After completing this session, you will be able to:

- Develop an understanding of the changing US and global legal and technical landscape in security and privacy
- Identify a business-driven plan to ensure solutions are keeping up with changes
- Understand the current legal environment
- Design solutions to ensure your organization and information is secure

233

Using Encryption Technologies to Protect Data

Alfred John Bacon, CISA, CISM, CRISC

Senior Consultant, Internal Controls
PETROBRAS

After completing this session, you will be able to:

- Understand the planning process for the use of data encryption technologies
- Grasp the required building blocks of a data encryption process
- Build threat models for each different instance of data protection
- Develop a plan to mitigate the risks identified in the threat modeling process
- Gain a clear view of the management decisions involved in using encryption
- Comprehend the risks involved in badly managed encryption solutions

243

Data Breach and Trade Secret Theft: How a Holistic Approach Can Protect Your Assets

William Hardin

Director
Navigant

Brad Pinne

Director
Navigant

After completing this session, you will be able to:

- Gain a perspective on applicable regulations and compliance requirements
- Understand the risk factors associated with data breaches and trade secret thefts

- Identify controls and data management best practices that help mitigate the risk
- Discover key considerations for creating and implementing an incident response plan
- Learn how IT can facilitate effective data breach and trade secret theft investigations

313

Developing and Deploying an Enterprise Strategy for Information Loss Prevention

Kevin Novak, CISM

Chief Information Security Officer and IT Risk Manager
Northern Trust

After completing this session, you will be able to:

- Draft a set of core requirements for your deployment
- Identify teams that need to be involved
- Engage in informed discussions about legal concerns/impacts (from a non-attorney perspective)
- Develop a solid understanding of your resource requirements
- Avoid pitfalls encountered by other organizations

323

Understanding and Mitigating System, Compliance and Legal Consequences of Cloud Computing

Michelle V. Crawford, CISA

Assistant Professor
Alabama State University

After completing this session, you will be able to:

- Understand the common terms and definitions of cloud computing
- Understand the business benefits and business considerations of cloud computing
- Recognize the compliance and legal consequences of cloud computing and its financial and strategic impact on an organization
- Explain typical steps of a risk assessment and/or audit review and understand the implications for organizations
- Understand the impact and changes of cloud computing on information security and/or audit plans

333

Reform of the European Union Data Protection Framework—A US Perspective

Charlie Blanchard, CISA, CISM, CRISC

Manager
Deloitte

After completing this session, you will be able to:

- Gain an understanding of the January 2012 European Commission's first draft of the EU Data Protection Framework
- Learn how the broadening of the scope—EU rules will apply if personal data is processed abroad—by all companies including those in the United States—that are active in the EU market
- Understand the single set of rules on data protection, valid across the EU and how it replaces the current patchwork of national rules in 27 member states
- Recognize the increased responsibility and accountability for those processing personal data
- Be familiar with the penalties of up to €1 million or up to 2% of the global annual turnover of a company for violations

413

A New Opportunity for IT Professionals: PS-Prep™ Audit

Lynnda M. Nelson,
Moderator

President
ICOR

James Nelson

President
Business Continuity Services, Inc.

Paul Burck

President
Orion

Marcus Pollock

Chief
Standards and Technology Branch (FEMA/DHS)

Kathy Glynn

Founder
GAP Resources

Timothy Woodcome

Director
Conformity Assessment, NQA-USA (Certifying Body)

Scott Richter

Director—Planning & Development
ANSI-ASQ National Accreditation Board

After completing this session, you will be able to:

- Understand the basics of the 3 new standards that measure business continuity program effectiveness and how they will impact the IT Auditor
- Understand the purpose of the Private Sector Preparedness initiative and how it relates to the organization
- Describe how to prepare the organization for the audit process for PS-Prep™ certification as both an internal auditor and an auditor consultant
- Share this information with the senior management team

Track 4 What's Around the Corner?

Enterprises understand that strong relationships between business goals and supporting processes are imperative to sustain organizational success. This track explores the concepts and terminology of issues related to IT governance, IT frameworks and IT risk management. Sessions will include concept discussions of ISACA research deliverables, new models and frameworks. Sessions combine practical business knowledge, examples and best practices to arm IT professionals with the resources and tools they need to navigate today's complex IT environment.

114

Emerging IT Risks Panel Discussion

Jill Farrington—Moderator

*Partner
KPMG LLP*

David Baker, CISA

*Sr. Manager, Professional Practices
Sara Lee*

Scott M. Shinnors, CISA

*Finance Director
ConAgra Foods Inc.*

After completing this session, you will be able to:

- Understand risks in cloud, big data, mobile devices and social media
- Develop processes to mitigate these risks

124

Emerging IT Risks Roundtable

Jill Farrington—Moderator

*Partner
KPMG LLP*

Mary Ann Stoltenberg-Smith, CISA, CISM, CRISC

*Vice President & IT Audit Manager
Federal Reserve Bank of Chicago*

David Baker, CISA

*Sr. Manager, Professional Practices
Sara Lee*

Scott M. Shinnors, CISA

*Finance Director
ConAgra Foods Inc.*

Join this interactive session for specific table discussions on cloud, big data, mobile devices and social media.

After completing this session, you will be able to:

- Understand the risks and practical approaches used by industry peers and organizations
- Benchmark your organization

134

A Lesson for Leaders: How to Attract and Retain Top Personnel in Today's Economy

Derek Duval

*Owner
Duval Search Associates*

After completing this session, you will be able to:

- Identify five critical questions in the hiring and selection process
- Understand how to implement an effective onboarding and employee recognition program that leads to engagement and productivity
- Create accountability for results
- Utilize critical communications required for engagement and retention

214

Changing the C-Suite Perception of Internal Audit

Princy Jain, CRISC—Moderator

PricewaterhouseCoopers

Linda Glaub

*Sr. Director Internal Audit
Citrix Systems, Inc.*

Scott Moreland, CISA, CRISC

*VP, Director of Internal Audit
Raymond James Financial*

Abhijit Pandit, CISA

*Director
Adobe Systems, Inc.*

Dan Williams

*Senior Vice President, Internal Audit
Darden*

After completing this session, you will be able to:

- Understand how internal audit is viewed today by the C-Suite
- Recognize the how landscape is changing
- Identify how Internal audit is a strategic partner of C-Suite
- Participate in case studies

224

Healthcare Security: Learning from Rigorous Government Security Requirements

Todd Fitzgerald, CISA, CISM, CGEIT, CRISC

*Director, Global Information Security
ManpowerGroup*

After completing this session, the participant will be able to:

- Leverage 11 years of government healthcare progressive security focus to develop a roadmap for your own healthcare organization
- Approach a government audit with preparation vs. surprise
- Apply NIST 800-53 standards to healthcare security
- Determine appropriate risk levels of audit issues
- Apply technical and non-technical security solutions to key problem areas

234

Mobile Device Security, Privacy, and Data Protection

Michael Davis

*Chief Executive Officer
Savid Technologies, Inc.*

After completing this session, you will be able to:

- Understand the top 10 mobile security risks and solutions to address each
- Realize privacy concerns with employees using their own mobile devices
- Understand how to assess an organization's unique mobile risks
- Recognize the various technologies used to reduce mobile security risk.
- Identify tips and techniques to audit a mobile security program
- Communicate and discuss mobile security risks with the organization

244

SAP: Real Time Controls in the SAP Environment

Steve Oberhauser, CISA

Senior Manager
KPMG

After completing this session, you will be able to:

- Understand Governance, Risk and Compliance in an SAP environment
- Comprehend SAP's GRC Access and Process Control
- Identify the new features and functionality provided in SAP GRC version 10
- Recognize the key settings to be reviewed and why
- Learn from the observations of recent implementations



Downtown Orlando

314

Data Security & Privacy: Can it Be Institutionalized?

Sophia Schell, CRISC

IBM

After completing this session, you will be able to:

- Creating Process to Balance Benefits & Potential Impacts
- Establishing Comprehensive Management System
- Fostering Security Conscious Culture
- Focusing on People Dimension with Organizational Change Practices
- Leveraging COBIT 5

324

Is IT Still Relevant? Communicating Trends and Risks Found in the New Technology Landscape

Robert E Stroud, CGEIT, CRISC

Vice President Strategy and Innovation
CA Technologies

After completing this session, you will be able to:

- Communicate the top industry trends in technology and communicate their impacts
- Understand where the ISACA guidance is located and how to use it
- Communicate the top industry risks with new technologies
- Apply ISACA guidance to one's role

334

Incident Management

Jeff Roth, CISA, CGEIT

Information Systems Assurance Engineer
Parsons

After completing this session, you will be able to:

- Identify incident detection and recording
- Recognize investigative techniques and diagnosis
- Determine resolution and recovery
- Establish and evaluate incident framework management

414

Understanding Your Data Flow: Using Tokenization to Secure Data

Ulf Mattsson

CTO and co-founder
Protegrity

After completing this session, you will be able to:

- Understand vulnerabilities and solutions for storing data in the cloud and outsourced environments
- Use a business risk approach to measure and position established and emerging data security options
- Implement a best practices approach to evaluate different options for data tokenization and encryption
- Understand data protection strategies and case studies for compliance with data security mandates
- Review case studies to gain understanding on how to stay out of scope for PCI DSS
- Communicate and report data protection cost efficiency with different approaches

424

How to Protect Your Network when Social Media Drives Malware Delivery Vehicle

Paul Henry

Security Analyst and Forensic Expert
Lumension

After completing this session, you will be able to:

- Implement a solid defense strategy against the excessive malware trends exploding within social networking platforms
- Determine how to employ reliable protection security methods when utilizing social media technologies in the enterprise
- Understand the necessary actions needed to immediately enhance an organization's security posture, without having to make new technology investments or prohibit employees' use of social networking tools
- Recognize the various malware attack campaigns within various social media platforms and how to avoid these evolving risks

Track 5 Managing IT Governance and Compliance Issues

Both topics provide perspectives on IT issues at the strategic level enabling managers to make well-informed planning and resource decisions. This track covers two related topics:

IT Governance: IT governance encompasses all stakeholders, and internal and external customers, and partners in the decision-making process, and subsequent monitoring to ensure risk-return value is delivered to the organization. Enterprise objectives are achieved by evaluating stakeholder needs, setting direction and monitoring performance to ensure risk-return value is delivered to the organization. This track covers governance as it relates to the IT investment portfolio, program management and operational controls for service delivery.

IT Compliance: This topic explores a variety of specific regulations and contractual compliance requirements, and the impact of regulatory compliance and how IT affects the entire organization. Session discussion will include the impact of compliance on controls and specifically the importance of integrating technology objectives into the overall business strategy.

115

IT Governance Considerations with Mobile Computing

Phil Lageschulte, CGEIT
Partner
KPMG

Martin Sokalski
IT Audit Manager
KPMG LLP

After completing this session, you will be able to:

- Understand the benefits and impact of mobile computing and Bring Your Own Device (BYOD)
- Understand the threat landscape of mobile computing
- Develop a mobile computing policy and governance structure
- Assess and mitigate mobile computing risks

125

Regulator Hot Topic Panel

Panel of Industry Experts

135

Trends in Compliance and Regulations

Panel of Industry Experts.

215

Implementing COBIT Quickstart in a Healthcare Organization

Nelson Gibbs, CISA, CISM, CGEIT, CRISC
Consultant

After completing this session, you will be able to:

- Contrast COBIT and COBIT Quickstart to help identify when Quickstart may be appropriate for deployment
- Define a roadmap for COBIT Quickstart implementation
- Recognize where COBIT Quickstart needs to be supplemented to meet regulatory requirements
- Understand how to use COBIT Quickstart as a preliminary step in deploying a more comprehensive control framework

225

Data Quality and Data Classification-Comparisons, Efficiencies and Success Factors

Gary Alterson, CISA, CRISC
Senior Consultant
Neohapsis

After completing this session, you will be able to:

- Identify the differences in data quality and data classification initiatives
- Articulate external regulatory drivers for both data quality and data classification
- Understand key components of data quality initiatives
- Explain key components of data classification initiatives
- Leverage synergies between data quality and data classification within data governance and information security programs

235

eDiscovery: Trends, Leading Practices, Risks, and Controls

Scott M. Shinnars, CISA
Finance Director, Internal Audit IT
ConAgra Foods, Inc.

After completing this session, you will be able to:

- Identify major areas of legal and regulatory risk related to poorly controlled data governance programs
- Clarify the nature and extent of the business, legal, and IT risks associated with ESI related to potential litigation
- Describe the elements of an effective e-Discovery risk management program
- Assist management with necessary steps to identify and mitigate the risks associated with e-discovery
- Articulate ways to improve data governance by leveraging existing organizational efforts related to compliance, data privacy, and information security
- Discuss the critical elements of an internal audit over the e-Discovery program

245

Healthcare Privacy and Security Landscape in 2012

Cliff Baker
Chief Strategy Officer
HITRUST Alliance

Todd Fitzgerald, CISA, CISM, CGEIT, CRISC
Director, Global Information Security
ManpowerGroup

After completing this session, you will be able to:

- Appreciate the current acceleration of security and privacy activities occurring in healthcare
- Understand the new regulatory developments and challenges including Stage 1— Meaningful use risk assessment and

expectations for Stage 2, accounting for disclosures

- Examine impact of Health Information Exchanges
- Prepare for expected enforcement activities —OCR proactive HIPAA Audits, CMS Audits, State Action
- Choose between compliance approaches such as SSAE-16, PCI for Healthcare, HITRUST Common Security Framework, Third Party/ Vendor/Business Associate Due Diligence

315

Certificates—
The New Authentication:
Risks and Remediation

Paul Turner

*Vice President, Product & Customer Solutions
Venafi*

After completing this session, you will be able to:

- Understand the critical role that SSL and SSH keys and digital certificates play in protecting mission-critical assets
- Describe the requirements and process flow to discover the population of keys and certificates
- Summarize the process of analyzing a key and certificate population to quantify the severity of an organization's risk
- Provide high-level overview and best practices for encryption asset lifecycle, key lengths and algorithms, and access control mechanisms for SSL and SSH keys and certificates that should be in place to mitigate the risks
- Identify the IT and InfoSec consequences of real-world case studies of worst case encryption key and certificate management practices
- Know where to obtain the high level information to organize a discovery and analysis.

325

Beyond Compliance: Reduce
Operation Risk and Cost While
Complying

Sven Skoog, CRISC

*Sr. Managing Consultant, Cybersecurity & Privacy
IBM*

After completing this session, you will be able to:

- Take the fear and uncertainty of compliance away to focus on benefits of cloud computing
- Reduce cost with a long term best practice approach
- Learn leading technology that help cut costs and reduce risk
- Discuss customer case studies



335

Review FFIEC Supplemental
Guidance on Internet Banking
Authentication, Combat Internet
Banking Risks

Russ Horn, CISA, CRISC

*COO
CoNetrix*

After completing this session, you will be able to:

- Recognize threats to Internet banking
- Understand new guidance associated with Internet banking
- Conduct an Internet banking risk assessment
- Identify compensating controls to reduce the risk of Internet banking
- Develop Internet banking policies
- Discover ways to educate customers on the risks of Internet banking

415

IT Governance: Myth to Reality

Michael Bargerhuff, CRISC

*Manager, IT Governance, Risk and Compliance
Ultimate Software*

After completing this session, you will be able to:

- Integrate the IT governance role into the strategic mission of the company
- Become a catalyst for strategic direction, maturity, optimization, and security
- Forge meaningful partnerships with security, risk, audit, and business departments
- Implement meaningful and compelling metrics to reflect governance health in real time
- Dramatically minimize overhead attributed to compliance and risk related functions
- Become the defacto 'go to' across the enterprise for consulting advice on new projects, initiatives, and enhancements

425

Information Warfare: Because
Weapons Aren't Always Made of
Steel

Brian Contos

*Director Global Security Strategy
McAfee*

After completing this session, you will be able to:

- Recognize several modern attack vectors
- Better understand the threats from the attacker's perspective after witnessing a demonstration of real-life hacks
- Analyze the nation-states and their supporters and sympathizers to expand the presentation beyond the technical issues and better understand the "who" and "why"
- Explore several case studies as they relate to the mitigation of advanced, targeted, attacks by aggressors with strong motivation as well as financial and technical means

Track 6 Top 11!—Top Audit and Security Issues

IT professionals in all business sectors are accountable for due care in handling information. It is now more important than ever for organizations to protect and maximize the value of intellectual property and manage risk. This track identifies today's top technology risks that are relevant to all IT assurance, risk, security or governance professionals. Sessions will identify the specific nature of these risks and how they impact the organization. Attendees will learn how to effectively evaluate risk and increase business value.

116

NEW for 2012: Emerging IT Audit Risks

Michael Juergens, CISA, CGEIT, CRISC
Principal
Deloitte

After completing this session, you will be able to:

- Identify the top 10 emerging technology risks that IT auditors must know now
- Understand the specific nature of these risks and how they can impact the business
- Know what tactical steps should be taken to manage and to mitigate these risks from an IT audit perspective
- Evaluate these risks allowing the IT audit function to drive more strategic value to the enterprise

126

System Authentication: The New Risk and 7 Steps to Audit and Remediate

Jeff Hudson
CEO
Venafi

After completing this session, you will be able to:

- Share some of the assessments performed at unnamed large institutions and discuss what was found
- Discuss how to obtain the information from an organization's network and perform the analysis to assess that organization's environment

136

Auditing Cloud Computing and Outsourced Operations

Mike Schiller, CISA
Director of Global Server, Database, and Storage Infrastructure
Texas Instruments

After completing this session, you will be able to:

- Perform audits of both cloud computing and other forms of outsourced IT operations
- Leverage a full understanding of terminology and definitions for cloud computing and other forms of IT outsourcing
- Understand a step-by-step audit approach and explanation of risks addressed

216

In the Crosshairs of Social Engineering Attacks

Eric Olson
Vice President of Product Strategy
Cyveillance, Inc.

After completing this session, you will be able to:

- Recognize the weaknesses of policies and technologies that allow criminals to circumvent these defenses
- Identify the educational shortcomings that allow personnel to be exploited
- Determine the latest vectors being exploited by sophisticated criminals
- Evaluate technologies today that can help protect against socially engineered attacks
- Outline best practices for protecting against socially engineered attacks

226

Secure Coding: Best Practices

Industry Expert

After completing this session, you will be able to:

- Determine whether an organization has a good secure coding practice
- Understand the OWASP Top 10 vulnerabilities
- Integrate OWASP Top 10 vulnerabilities into the secure coding practice
- Approach for performing secure code reviews
- Approach for developing a secure coding baseline
- Identify commercial and open source tools to help establish and maintain a secure coding practice
- Comprehend how to audit a secure coding practice

236

Reduce Cloud Security and Compliance Risks by Automating Privileged Accounts

Adam Bosnian
EVP Americas and Corporate Development
Cyber-Ark Software

After completing this session, you will be able to:

- Understand how to proactively and systematically reduce risk within cloud-based or virtualized environments around 'High Value Infrastructure Targets'
- Manage the security and audit challenges of shared administrative accounts and embedded application identities
- Recognize the potential return on investment from automated privileged account management
- Learn new technologies for securing, managing and updating critical accounts, including identities embedded in all applications across the virtual enterprise
- Manage the administrative and application accounts for thousands of applications, servers, network devices, and databases
- Discover how to ensure administrative and application identities and passwords are changed regularly, highly guarded from unauthorized use and closely monitored, including full activity capture and recording

246

Social Media Risk and Mitigation Guidance

Rumy Jaleel-Khan, CISA, CRISC

Senior Manager
Deloitte

Mike Wyatt, CISA

Director, Security and Privacy Services
Deloitte & Touche LLP

After completing this session, you will be able to:

- Identify social media vulnerabilities
- Develop risk assessment metrics to align the social media activities with the overall business objectives
- Recommend a social networking policy to increase employees' security awareness of information that can be shared over social networks.
- Review an audit program incorporating the risks
- Identify approaches to address social media risks and threats



316

Identify and Eradicate: The Top Security Threats to Banks in 2012

Russ Horn, CISA, CRISC

COO
CoNetrix

After completing this session, you will be able to:

- Identify the top information security risk to financial institutions
- Recognize trends in security threats to financial institutions
- Discover emerging security threats to financial institutions
- Conduct an information security risk assessment
- Explore recommendations to deal with current and future security threats
- Identify ways to educate employees and customers on information security

326

After the Breach

Ray Soriano, CISA, CISM, CRISC

Director
Deloitte & Touche LLP

After completing this session, you will be able to:

- Recognize the current limitations of legacy security controls in a cloud computing environment
- Overcome concerns with loss of control and visibility of data as it moves to cloud computing environments

336

How to Conquer the Social Media Landscape: The Vanguard Experience

Theodore H. Wolff, CISA

Senior Manager
Vanguard

After completing this session, you will be able to:

- Understand Vanguard's business case for social media
- Learn from Vanguard's experience in recognizing social media risk
- Experience the Vanguard journey to operationalize and sustain effective procedures to mitigate social media risk
- Gain insight from the audit of Vanguard's social media operation
- Discuss risk and reward opportunities with social media based on industry experiences

416

Protecting Your Mobile Devices

Nelson Gibbs, CISA, CISM, CGEIT, CRISC

Consultant

After completing this session, you will be able to:

- Analyze the evolution towards mobile computing
- Identify key risks for mobile devices
- Describe the architecture of common mobile operating systems including Android and iOS
- Explain strategies and techniques for securing mobile devices
- Discuss resources available to plan and perform a mobile device audit

426

WikiLeaks: Are You the Next Target?

Richard Payne, CISM, CGEIT, CRISC

Associate Partner
IBM Business Consulting Service

After completing this session, you will be able to:

- Identify the information security failures that allowed US Government secrets to be stolen
- Define an effective controls strategy that mitigates the risks of data theft
- Determine what assets within their own organization represent attractive targets for thieves
- Evaluate the "size of market" for stolen data, and the agendas that drive the WikiLeaks community
- Defend organizations against "insider threat"

Track 7 Managing Risk and Exposure

This track provides the knowledge required to help IT professionals advance their arsenal of skills needed to perform more advanced tasks and expand upon their job responsibilities. It will cover a variety of topics including using COBIT® and COSO to understand, identify, and assess IT risks, and how to use internal control frameworks to mitigate risks. Sessions provide guidance to help IT professionals translate complex IT related risk scenarios into IT tactics that are relevant to all business units across the organization. Attendees will explore concepts of risk management and how to effectively apply them to make better business decisions and maximize the trust in, and value from, information technology.

117

Enterprise Risk Management Essentials

James Ambrosini, CISA, CRISC

*Director
Protiviti*

After completing this session, you will be able to:

- Understand the difference between ERM and typical risk management activities
- Learn fundamental concepts for a successful ERM implementation
- Walk through a case study from a company implementing ERM in a high-risk industry and examine their methodology and artifacts
- Understand how organizational risk affects companies' risk tolerance, and what to look out for, by examining a classic case of risk management failure

127

IT Risk Management Life-cycle and Enabling IT with GRC Technology

Debbie Lew, CISA, CRISC

*Senior Manager
Ernst & Young, LLP*

Steven F. Jones

*Senior Manager
Ernst & Young LLP*

After completing this session, you will be able to:

- Gain an understanding of the key components of a comprehensive risk management program



- Gain an understanding of the IT risk management life cycle to identify, assess, monitor and report on IT-related risks including identifying opportunities to improve or optimize
- Determine types of enablers available including COBIT and Risk IT to facilitate the IT risk assessment process including awareness of how technology can operationalize risk management processes
- Obtain an overview of GRC technology, industry landscape, business drivers, benefits, trends and challenges
- Gain an understanding of how technology can be used to enable IT risk management processes to potentially reduce the cost of IT risk management, compliance and audit, streamline reporting, better manage risk, and deliver insight for better decision making.

137

Reduce IT Risk through Improved Management and Planning

Gary Alterson, CISA, CRISC

*Senior Consultant
Neohapsis*

After completing this session, you will be able to:

- Articulate how IT risk management supports ERM objectives
- Develop an IT risk universe that supports business decision making
- Design a risk taxonomy that enables comparable and common representations of risk
- Facilitate a continuous IT risk assessment and remediation planning process grounded in Risk IT

217

The Opportunity in Risk and Security Trends

Tom Patterson, CISA, CGEIT, CRISC

*Associate Partner
IBM Global Services*

After completing this session you will be able to:

- Understand why new domains require more information aggregation and sharing across organizations
- Address challenges to protecting information and complying with restrictions on data use
- Recognize the risks associated with the failure to protect and secure sensor event data are far higher than the risks usually associated with IT event data
- Learn how and why each industry domain has developed their standards independently, challenging the ability to integrate command and control operations
- Identify critical decisions in real time
- Distinguish how to make decisions instantly, especially in a crisis, depends on real time monitoring and tracking of people and high value assets which can be abused and attacked

227

What Color is Your Information Risk Today?

Jim Hurley

*Managing Director, IT Policy Compliance
Symantec Corporation*

After completing this session, you will be able to:

- Understand why finding answers to "What color is our information risk—today?" is the most important question
- Document the practices of organizations that are able to answer this question today
- Evaluate the index for brand, reputation, headline, revenue and customer retention risks for their own organization and be able to explain it to colleagues
- Identify and evaluate practices in their own organization that will most reduce the risks
- Leverage interactive self-assessments after the conference to align change in your organization and cope with waves of "information anywhere"



NACACS 2011 Networking Event

327

SaaS: How to Secure the Services Your Team Provides

Michael Davis
Chief Executive Officer
Savid Technologies, Inc.

- After completing this session, you will be able to:
- Recognize how firms are transitioning security or audit teams to provide a menu of services
 - Understand the business need and how the services are used
 - Manage the team as a service provider

337

CFO and CIO: Partners or Opponents?

Daniel Dec, CISA, CISM
Principal Consultant
Cognizant Technology Solutions

- After completing this session, you will be able to:
- Understand the priorities of a CFO and a CIO, and recognize the different scenarios for alignment
 - Comprehend how CFOs and CIOs each perceive technology risk
 - Recognize the perspective of compliance requirements from a CFO and a CIO's lens
 - Learn how third party risks affect the office of CFO and office of CIO
 - Realize how the CFO and CIO, working together, deliver and sustain a compliant and secure IT environment

417

How to Make Enterprise Governance Risk and Compliance (eGRC) Work for You

Kevin Novak, CISM
Chief Information Security Officer and IT Risk Manager
Northern Trust

- After completing this session, you will be able to:
- Clearly articulate how eGRCs can be used to complement an enterprises IT Risk Management program
 - Integrate IT Risk into an Enterprise Corporate Risk framework
 - Clearly articulate goals and objectives for an effective eGRC strategy
 - Bring the right teams to the table for planning a long term eGRC strategy, and keeping those teams engaged
 - Estimate resource requirements for supporting an eGRC program
 - Avoid some pitfalls encountered by other organizations while planning and deploying an eGRC

237

Security Auditing and Governance for Healthcare Providers

Tom Turo, CISM, CRISC
Information Security Manager
Adventist Health System

Sharon Finney, CISM
Corporate Data Security Officer
Adventist Health System

Steve Stallard
CISO
Orlando Health

Christi Rushnell
VP Information Technology
Health First

- After completing this session, you will be able to:
- Learn methods for deploying sound security policies and guidelines
 - Acquire tools used for security training and awareness
 - Understand auditing methods of end users on need to know
 - Discover risk assessments of providers and the continuous improvements to reduce risk
 - Develop automated auditing methods and custom templates
 - Ascertain remediation processes

247

Black Holeistic Disaster Recovery: How to Limit Losses

Donald Gallien, CISA, CISM
Vice President, Audit Leader
American Express

David Maberry
Chief Risk Officer
American Fidelity Assurance Company

- After completing this session, you will be able to:
- Engage executives with meaningful BCP/DR audit issues
 - Identify and report BCP issues the executives will care about
 - Apply practical audit steps for identifying inherently flawed business continuity and disaster recovery plans
 - Message BCP and DR issues with impact
 - Complete "Sell the Chief Risk Officer" case studies

317

Establish & Maintain Information Security Oversight

Daniel Dec, CISA, CISM
Principal Consultant
Cognizant Technology Solutions

- After completing this session, you will be able to:
- Establish a sustainable information security governance program within a MSP model
 - Understand how effective oversight increases effectiveness of security programs
 - Utilize KPI and KRI's to show incremental performance and risk management progress
 - Leverage metrics to understand and articulate segmented risk profiles

NACACS 2012 Workshop Descriptions

All sessions are recommended for professionals with 3 or more years of IT experience and a working knowledge of IT terminology.

Pre-Conference

WS1

Control and Security of Web Applications *(two day)*

Kevin Nibler

*Senior Manager, Security and Audit Services
Canaudit Inc.*

As web applications quickly grow more common, complex and critical they increasingly become easy, lucrative targets for attackers and a growing risk to the organizations that employ them. In order to assess, manage and mitigate this risk, IT auditors must understand: how web applications work, how they are being leveraged by malicious individuals and what controls can be implemented to minimize organizational risk.

This workshop will provide attendees a hands-on glimpse at the technologies under the hood of today's web applications, so they know how they operate, hands-on examples of common vulnerabilities, so they understand their risk and exposure, discussion of controls, so they understand proper mitigation and risk control tables and a practice audit so they can return to their organization's confidence in their ability to independently perform a basic web application penetration test and vulnerability assessment. This session will heavily reference OWASP's list of the Top 10 Most Critical Web Application Security Risks, include case studies of high profile breaches and examples and cover basic concepts such as HTML, JavaScript, PHP, ASP, SQL, session IDs, and cookies.

After completing this workshop, you will be able to:

- Understand modern web application architecture
- Understand and explain the risk and exposure of the today's top web application security risks (OWASP Top 10)
- Understand the controls needed to mitigate today's top web application security risks
- Perform basic web application penetration tests
- Use provided risk/control tables to perform basic web application vulnerability assessments

WS2

IT Risk Management *(two day)*

Shawna M. Flanders, CISA, CISM, CRISC

*Productivity Specialist
PSCU-FS*

This workshop is designed to provide valuable information and hands-on experience for both IT risk professionals and IT auditors.

This two-day workshop describes the principles of IT risk management, the responsibilities and accountability for IT risk, how to build up awareness, and how to communicate risk scenarios, business impact and key risk indicators utilizing ISACA's Risk IT framework and the process model that includes risk governance, risk evaluation, and risk response. The workshop will explain how ISACA's Risk IT framework relates to COBIT and how it can help to achieve best practices in IT risk management. The workshop will provide practical guidance on how to integrate IT risk management into ERM, establish and maintain a common risk view, and make risk-aware business decisions and how to maintain an operational risk profile, assess and respond to risk, as well as how to collect event data, monitor risk, and report exposures and opportunities.

After completing this workshop, you will be able to:

- Apply key deliverables necessary to develop and maintain an effective risk management program following the Risk IT Framework
- Explain how the new Risk IT framework relates to COBIT
- Evaluate implementation and operational issues
- Integrate IT risk management with ERM
- Audit/Evaluate the risk management program

WS4

Performing IT Audits: A Practical Approach *(one day)*

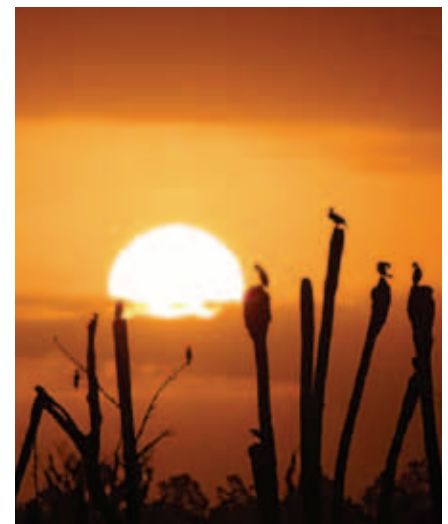
Phil Flora, CISA

*Principal
FloBiz & Associates, LLC*

This workshop will include the primary aspects of how to conduct a risk-based IT audit using professional standards and will also include all parts of the audit engagement: planning, fieldwork, reporting and a high-level overview of the annual risk assessment process. During the workshop you will receive a hands-on sample of performing an IT audit. The participant activities will provide real life examples to reinforce the learning concepts. Performance of the audit activities will result in determining the efficiency and effectiveness of the identified operations, processes, programs, projects and initiatives based on the audit objectives.

After completing this workshop, you will be able to:

- Understand the relationship between annual risk assessment and engagement planning
- Learn to develop audit objectives
- Develop audit programs that identify the primary risk areas based on the allocation of limited audit hours
- Practice key elements of the audit process
- Establish a focused testing plan for primary process controls
- Summarize the audit results to communicate effectively with management



Everglades

WS5

Server Virtualization Security and Audit *(one day)*

Michael T. Hoelsing, CISA
Faculty
 University of Nebraska at Omaha

(Updated for 2012 and returning as one of 2011's highest rated workshops.)

Virtualization is the tool that has created fluidity in the IT server infrastructure. This has enabled new approaches to data center compilation (public cloud, private cloud). This course is designed to give the auditor a background in server virtualization, the risks associated with that implementation, control or security techniques to mitigate those risks, and approaches, tools, and techniques to gather evidence to assure that those controls and security tools are working as intended.

*****Laptops Required for this workshop.*

After completing this workshop, you will be able to:

- Recognize risk and controls that are unique to a virtualized server environment
- Recognize the risks and controls that carry over from the physical server world, maybe in a different form, to the virtual server environment
- Develop standards documents and audit programs based on industry guidance from vendors (VMware), government (DISA), and independent organizations (Center for Internet Security)
- Customize an audit program based on a draft 17 page example program that will be provided to participants
- Identify assessment tools applicable to virtualization, including free tools and commercial tools
- Apply manual assessment/evidence-gathering techniques to a live virtual server and management console
- Run basic assessment tools against a virtualized server and understand the components tested, or not tested and how the evidence was gathered (proprietary and public domain protocols such as XCCDF)
- Assess the future direction of virtualization architecture (ESXi without a console operating system) and its impact on risk, controls and assessment procedures
- Map testing procedures to a current compliance standard such as PCI/DSS

Post-Conference

WS6

Cloud Computing Audit and Assurance Issues *(one day)*

Dan Cimpean, CISA, CGEIT
Partner
 Deloitte Enterprise Risk Services

Cedric Lempereur, CISA, CISM
Senior Manager
 Deloitte

(Updated for 2012 and returning as one of 2011's highest rated workshops.)

In performing their activity, risk managers, IT auditors or security managers face challenges in defining a framework that covers the main security information assurance topics implied by cloud computing. A number of frameworks have been developed and can serve as a basis for further cloud computing risk identification and assessment. A good preparation and understanding of challenges ahead will allow professionals to provide value-added, concrete and actionable recommendations to be applied.

After completing this workshop, you will be able to:

- Identify key trends in cloud computing from an assurance perspective
- Discuss current and emerging risks related to the use of cloud computing
- Define a cloud computing Information Assurance Framework (CCIAF)
- Address cloud computing risks starting with the Assurance Framework

WS7

Data Loss Prevention

Kyle Harvey, CISA
IT Risk and Assurance Manager
 Ernst & Young LLP

Chip Wentz, CISA, CISM, CGEIT
Senior Manager—Advisory Services
 Ernst & Young LLP

Confidential client data, internal financial details, organizational strategies and intellectual property, are crucial to organizations integrity. Preservation of this data is vital; failure to do so has an impact on organizational reputation and may also incur financial consequences. Today data is expanding and changes exist in where data resides.

After completing this workshop, you will be able to:

- Understand data loss requirements
- Design a policy and program that works for your organization
- Manage your compliance requirements



Loews fountain

Program Benefits

Your North America CACS registration fee includes:

- Attendance at the conference sessions of your choice
- An opportunity to earn up to 44 continuing professional education (CPE) credit hours
- Complimentary continental breakfast for conference attendees
- Complimentary lunches
- Complimentary morning and afternoon refreshment breaks
- Unlimited entry to the Solution Center
- Invitations to all social and networking events:
 - Welcome Reception
 - Solution Center Reception
 - Networking Reception

Pricing

Register by 16 March 2012 and save US \$200 on registration fees.

Conference	Member	Nonmember
Register on or before 16 March 2012:	US \$1,550	US \$1,750
Register after 16 March 2012:	US \$1,750	US \$1,950

Pre- and Post-Conference Workshops	Member	Nonmember
One-day Workshop	US \$550	US \$750
Two-day Workshop	US \$750	US \$950

If your organization plans to register four or more individuals for 2012 NACACS, you may be eligible for a group discount. Please contact conference@isaca.org for additional information.

Register online at: www.isaca.org/2012NACACS or to register by mail or fax, download the registration form at: www.isaca.org/NACACSregistration

Venue Information

Whatever you can dream, Orlando can provide. Holding a conference in Orlando means more than a mere gathering. The city is known for its easy accessibility, famous year-round warm climate, true southern hospitality and unsurpassed accommodations, which makes it no surprise that Orlando was recently named the top US conference destination.

Stay in the heart of the conference action at a discounted hotel price. Accommodations are limited; please contact the hotel directly.

Loews Royal Pacific Resort at Universal Orlando®

6300 Hollywood Way, Orlando FL 32819
Toll-Free Reservations: +1.888.430.4999
Phone: +1.407.503.3000 (Ask for reservations department)
Fax: +1.407.503.3010
Web site: www.loewshotels.com

Guest Room Rate: \$179 Single/Double (US \$25 each additional occupant)

Rates based on availability

Guest Room Cut-off date: 20 April 2012

Group Discount Code: GP25U1

If you are booking your accommodations through www.loewshotels.com, please select "group" in the "partner/group rate" window before entering the group discount code.

Special Events

Welcome Reception

Sunday, 6 May 2012 | 5:30pm–7:30pm

Join us for the opening event of North America CACS. A highly interactive environment in an informal setting, this is an ideal time to begin networking with your peers and engage with many of the speakers. Do not miss this opportunity to reunite with friends and colleagues from around the world, and meet seasoned professionals as well as newcomers.

Solution Center Reception

Tuesday, 8 May 2012 | 5:00pm–6:30pm

The Solution Center Reception marks the official opening of the *InfoExchange*. Interact with exhibitors and continue to network with peers while exploring the newest products and services available to IT professionals. Exhibitors will be available to demonstrate products and answer questions. Join us for this valuable event.

Networking Reception

Wednesday, 9 May 2012 | 6:00pm–8:00pm

Tropical fun, sunshine and YOU!

Unwind with us at the North America CACS Networking Event for a few hours of relaxation, food, drinks and entertainment poolside at the Loews Royal Pacific. Be a part of the tropical décor and wear your favorite (or least favorite) tropical shirt for a chance to win some fun prizes! Stay for the grand prize drawing of a complimentary registration to the 2013 North America Conference in Dallas, Texas!

Spotlight Educational Sessions

Tuesday, 8 May 2012 | 5:15pm–6:30pm

Wednesday, 9 May 2012 | 10:15am–12:15pm

Interact with the exhibitors and earn CPE hours. ISACA offers special one-half-hour sessions presented by the *InfoExchange* exhibitors. Spotlight Educational Sessions provide an additional in-depth opportunity to interact with the exhibitors or see a demonstration about the products and services. Specific sessions and times will be announced at the conference.

Registration Methods

Choose one of four easy ways to register:

1. **ONLINE** at www.isaca.org/2012nacacs
2. **FAX** your completed registration form to +1.847.253.1443
3. **MAIL** your completed registration form to:
ISACA
1055 Paysphere Circle
Chicago, IL 60674 USA
4. **BANK WIRES**
send electronic payments in US dollars to:
Bank of America
135 S LaSalle St., Chicago, Illinois 60603
ABA #0260-0959-3
ISACA Account #22-7157-8
S.W.I.F.T. code BOFAUS3N

[Please include attendee's name and NAC2012 on the Advice of Transfer.]

Permission to be Photographed

By attending this event, the registrant grants permission to be photographed during the event. The resultant photographs may be used by ISACA for future promotion of ISACA's educational events on ISACA's web site and/or in printed promotional materials, and by attending this event, the registrant consents to any such use. The registrant understands any use of the photographs will be without remuneration. The registrant also waives any right to inspect or approve the aforementioned use of any photographs now or in the future.

Registration Dates and Hours

Preconference Workshop Registration

Saturday, 5 May, 7:30am–5:00pm
Sunday, 6 May, 7:30am–5:00pm

Conference Registration

Sunday, 6 May, 3:00pm–7:30pm
Monday, 7 May, 7:00am–5:00pm
Tuesday, 8 May, 7:30am–5:00pm
Wednesday, 9 May, 8:00am–5:00pm

Postconference Workshop Registration

Thursday, 10 May, 8:00am–5:00pm
Friday, 11 May, 8:00am–12:00 Noon

Cancellation Policy

If your plans change and you won't be able to attend the conference and/or workshop, contact us by phone, fax or email to cancel your registration. All cancellations must be received by **11 April 2012** to receive a refund of registration fees. A cancellation charge of US \$100 will be subtracted from conference refunds, and US \$50 from workshop refunds. No refunds can be given after **11 April 2012**. Attendee substitution is permitted at any time until the conference. If a non-member is substituting a member, then there will be additional nonmember fees.

NOTE: Registration is contingent upon full payment of the registration fee. To guarantee registration, conference and/or workshop fees must be received by the published deadline. It may take 10 or more business days for a wire transfer or mailed check to reach ISACA, so please plan accordingly. If, for any reason, ISACA must cancel a course or event, liability is limited solely to the registration fees paid. ISACA is not responsible for other expenses incurred, including travel and accommodation fees. Conference materials are not guaranteed to those who register onsite or fail to submit payment prior to the event. For more information regarding administrative policies, please contact the ISACA conference department.
Phone: +1.847.660.5585
Fax: +1.847.253.1443
Email: conference@isaca.org

Continuing Professional Education Credits

To maintain Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and/or Certified in Risk and Information Systems Control™ (CRISC™) certifications, certification holders are required to earn a minimum of 20 continuing professional education (CPE) credits annually and 120 CPE credit hours over a three-year period in accordance with ISACA's CPE policies. Attendees can earn up 44 CPE credits; 23 by attending the Conference and an additional 7 for each day of optional workshops.



ISACA conferences are Group Live and do not require any advanced preparation. ISACA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, www.learningmarket.org.

Dress

Business casual is appropriate for the North America CACS Conference and all conference events.

Register online now:
www.isaca.org/2012nacacs

Registration Form

1. Fill in the information below in block letters.

Name (Mr., Mrs., Ms., Miss) _____
(First/Given Name) (Middle Name) (Last/Family Name)

Title _____ Company Phone _____

Company _____ Company Fax _____

Badge Name (first name or nickname) _____ Email Address _____

Company or Home address (please indicate) This is a change of address.

Address _____

City _____ State/Province _____ Zip/Postal Code _____ Country _____

Permission to appear on attendee roster

Yes No

By selecting **Yes** you are agreeing to appear in the printed roster that is provided to our attendees, speakers and exhibitors at the conference, which includes your name, company name (if applicable) and country of residence, it will not display your e-mail address or any other contact information.

Permission to share contact information with sponsors/exhibitors Yes No

By agreeing to share your contact information, you help support our conference sponsors/exhibitors. Robust support of ISACA conferences by sponsors and exhibitors helps keep conference fees affordable for our attendees.

Your name, business address, professional title, current professional activity, size of organization, field of employment and email address will be provided to sponsors/exhibitors (when present). All sponsors/exhibitors are required to honor your request to opt-out of any further contact beyond the initial one.

ISACA member?

Yes.

Member number _____

No.

Become a Member and Save!

Nonmembers, start enjoying the benefits of ISACA membership today. The difference between member and nonmember conference fees can be applied towards ISACA membership, potentially enabling you to become a member at the international and chapter level for no additional cost. This offer expires 30 days after completion of the event. Don't miss this opportunity—apply today!

If you would like to take advantage of this offer, check the box below.

I wish to apply the difference between member and non-member conference fees towards ISACA membership. I have read and agree to the following membership disclaimer: By applying for membership in ISACA, members agree to hold the association and its chapters, and the IT Governance Institute, and their respective officers, directors, members, trustees, employees, and agents, harmless for all acts or failures to act while carrying out the purposes of the association and institute as set forth in their respective bylaws, and they certify that they will abide by the association's Code of Professional Ethics (www.isaca.org/ethics).

NOTE: This offer expires 30 days after completion of the event. Non-members pay the non-member conference fee when registering.

2. Circle your session choices (no more than one session per time period, please.)

Making session selections now does not restrict you from making changes or attending the session of your choice on-site.

Pre-conference Workshops														Post-conference Workshops	
Sat., 5 May 2012	Sun., 6 May 2012	Monday, 7 May 2012			Tuesday, 8 May 2012				Wednesday, 9 May 2012			Thursday, 10 May 2012		Fri., 11 May 2012	
9:00 AM–5:00 PM	9:00 AM–5:00 PM	10:15–11:45 AM	1:30–3:00 PM	3:30–5:00 PM	8:30–10:00 AM	10:30 AM–12 Noon	1:30–3:00 PM	3:30–5:00 PM	8:30–10:00 AM	1:30–3:00 PM	3:30–5:00 PM	8:30–9:45 AM	10:00–11:15 AM	1:30–5:00 PM	8:30–12 Noon
WS1		111	121		211	221	231	241	311	321	331	411	421	WS6	
WS2		112	122	132	212	222	232	242	312	322	332	412			
WS3		113	123		213	223	233	243	313	323	333	413			
WS4	WS5	114	124	134	214	224	234	244	314	324	334	414	424	WS7	
		115	125	135	215	225	235	245	315	325	335	415	425		
		116	126	136	216	226	236	246	316	326	336	416	426		
		117	127	137	217	227	237	247	317	327	337	417			

Registration Form Page 2 of 2

Attendee Name _____

3. Registration Fees (in US dollars subject to applicable VAT)

Conference Registration

Register by 16 March 2012 to save US \$200 on registration fees!

	Total
Member early-bird	US \$1,550
Nonmember early-bird	US \$1,750
Member (after 16 March 2012)	US \$1,750
Nonmember (after 16 March 2012)	US \$1,950

Pre- and Postconference Workshop Registration

	Total
One-Day workshop	
Member	US \$550
Nonmember	US \$750
Two-Day workshop	
Member	US \$750
Nonmember	US \$950

TOTAL (Add all circled above plus any additional item fees.) US \$ _____

ISACA offers discounts to organizations sending 4 or more employees to a single conference. Please contact the ISACA Conference department for more details at +1.847.660.5585 or conference@isaca.org.

4. Indicate Method of Payment

Payment enclosed. Make check payable to "ISACA" in US dollars, drawn on a US Bank.

Wire Transfer in US \$ _____ Date Transferred _____
Wire transfers and mailed cheque may take 10 or more business days to reach ISACA, so please plan accordingly.

Charge my Visa MasterCard American Express Diners Club

(NOTE: All payments by credit card will be processed in US dollars.)

Credit Card # _____ Expiration Date _____

Name of Cardholder _____

Signature of Cardholder _____

VISA

Obtaining a VISA is solely the responsibility of the registrant. Please contact the local government of the host country for details. Once a paid registration is received, a letter of invitation will be provided by ISACA, upon request.

5. Registration Methods

- A.  REGISTER ONLINE at www.isaca.org/2012nacacs
- B.  FAX your completed registration form to +1.847.253.1443.
- C.  MAIL your completed registration form to:
ISACA
1055 Paysphere Circle
Chicago, IL 60674 USA
- D.  BANK WIRES Send electronic payments in US dollars to:
Bank of America
135 S LaSalle St., Chicago, Illinois 60603
ABA #0260-0959-3
ISACA Account #22-7157-8
S.W.I.F.T. code BOFAUS3N

[Please include **attendee's name** and **NAC2012** on the Advice of Transfer.]

6. Cancellation Policy

If your plans change and you won't be able to attend the conference and/or workshop, contact us by phone, fax or e-mail to cancel your registration. All cancellations must be received by **11 April 2012** to receive a refund of registration fees. A cancellation charge of US \$100 will be subtracted from conference refunds, and US \$50 from workshop refunds. No refunds can be given after **11 April 2012**. Attendee substitution is permitted at any time until the conference. If a non-member is substituting a member, then there will be additional non-member fees.

NOTE: Registration is contingent upon full payment of the registration fee. To guarantee registration, conference and/or workshop fees must be received by the published deadline. It may take 10 or more business days for a wire transfer or mailed check to reach ISACA, so please plan accordingly. If, for any reason, ISACA must cancel a course or event, liability is limited solely to the registration fees paid. ISACA is not responsible for other expenses incurred, including travel and accommodation fees. Conference materials are not guaranteed to those who register onsite or fail to submit payment prior to the event. For more information regarding administrative policies, please contact the ISACA conference department.

Phone: +1.847.660.5585

Fax: +1.847.253.1443

Email: conference@isaca.org

Your contact information will be used to fulfill your request, and may also be used by ISACA to send you information about related ISACA goods and services, and other information in which we believe you may be interested. By registering, you authorize ISACA to contact you at the address and numbers you have provided, including to provide you with marketing and promotional communications. You further represent that the information you provided is yours and is accurate. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at www.isaca.org. If you elect to attend one of our events or purchase other ISACA programs or services, information you submit may also be used as described to you at that time.

7. Special Arrangements

Special Dietary Requirements _____

I will require assistance. Please contact me to make the necessary arrangements.