



North America Computer Audit, Control and Security Conference

18-22 April 2010
Hyatt Regency Chicago
Chicago, Illinois, USA



- Learn from industry experts
- Network with an unmatched group of peers
- Choose to attend sessions from 7 different tracks
- Earn up to 44 CPE hours

www.isaca.org/nacacs

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

If knowledge is power,
how powerful are YOU?



Get the knowledge you need to stay one step ahead of the competition and keep up with changing professional trends at ISACA's **North America Computer Audit, Control and Security** (North America CACSSM) Conference. North America CACS is the must attend, hot-topic event for IT audit, security, risk and governance professionals in North America. It attracts the best and brightest with its content-rich and thought-provoking sessions that delve into some of the biggest challenges facing IT audit and security professionals. Sessions focus on the latest approaches to address these challenges from business, managerial and operational perspectives, as well as new technologies and system approaches while identifying risks and opportunities. Reflective of ISACA's high standards, speakers are industry experts from all over the world. We know your time is valuable; North America CACS makes the most of your time away from the office, and your training dollars. To get the same quality of information you would have to attend several different events, and spend more time and money.

Immerse yourself in an environment that stimulates learning. Network with an unmatched group of peers. Return to the office, motivated to improve the organization and immediately apply the information you learned. **Attend North America CACS, a trusted educational forum where like-minded professionals can collaborate and connect.**

What's in it for you?

- **Customized learning experience.** Make the most of your time away from the office. Choose to attend the sessions that matter most to you and your enterprise and get information that can be put to use immediately when you return to the office.
- **World-class networking opportunities.** Interact face-to-face with like-minded individuals and enjoy an ideal environment for unparalleled knowledge sharing.
- **Update your knowledge.** Be the first to find out what's going on at ISACA. Get a sneak peek of new research and projects being developed, and broaden your understanding of what's going on around the world.
- **Sharpen your skills.** Expand your expertise. Earn valuable CPE hours.

What's in it for your organization?

- **Exceptional value for training dollars.** Attendees receive valuable reference materials from every session that can be shared with colleagues when they return to the office.
- **Exclusive access to industry experts.** Get tried and tested solutions to problems facing your organization from those who have been in your role before. Discover what works and doesn't work from experienced and successful professionals.
- **Interact with leading vendors.** Find all your organization's vendors in one place at the *InfoExchange*. Get answers to questions directly from vendors. Discover new products that will decrease the expense to your organization and increase the return.

KEYNOTE ADDRESS



Cynthia Cooper

Cynthia Cooper is an internationally recognized speaker on ethical leadership, the current economic crises and recent scandals. She was named one of *Time* magazine's Persons of the Year in 2002 and is one of only seven women who have ever received that distinction.

Cooper's presentation, titled *Ethical Leadership in the 21st Century*, will feature observations from her time at WorldCom, where she and her team unraveled one of the largest corporate frauds in history.

Currently, she is CEO of The CooperGroup, a firm that offers advisory and consulting services in the area of ethics and compliance, risk management, fraud prevention and detection, and internal audit. She is also the author of *Extraordinary Circumstances*, which discusses her experiences as a corporate executive and was called "one of the ten best of the best business books of 2008" by *The Globe and Mail*.

For more information, please visit the web site: www.isaca.org/nacacs.

Prerequisites

- B** – Unless otherwise noted for basic level sessions, the participant should have at least one year of experience and knowledge in this subject.
- I** – Unless otherwise noted for intermediate level sessions, the participant should have at least three years of experience and knowledge in this subject.
- A** – Unless otherwise noted for advance level sessions, the participant should have at least five years of experience and knowledge in this subject.

THANKS TO OUR GOLD SPONSORS:



Track 1—IT Audit Core Competencies

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
111	IT Security Control Frameworks and Standards Overview B	Todd Fitzgerald, CISA, CISM, CGEIT <i>Senior Technical Compliance Advisor</i> National Government Services	<ul style="list-style-type: none"> • Understand an overview of HIPAA, ARRA, GLBA and FISMA legislation • Be familiar with CoBIT®, Val IT™ and ISACA's Business Model for Information Security at an introductory level • Examine the applicability of PCI, ISO 27001/2, NIST 800-53, CoBIT, ITIL, and CMMI controls • Recognize common pitfalls and how to avoid them
121	IT Audit Fundamentals I	<p>Andy Cataldo, CISA <i>Technology Audit Manager</i> Estee Lauder Companies, Inc.</p> <p>Janak Master Estee Lauder Companies, Inc.</p> <p>Lorraine Peoples, CISA <i>Vice President—Internal Control Department</i> Estee Lauder Companies, Inc.</p>	<ul style="list-style-type: none"> • Develop and maintain the lifecycle of an audit • Understand how to plan, execute and create work-paper wrap up • Report findings and necessary follow-up to management • Understand general computer controls testing including system development life cycle (SDLC) • Understand general application controls testing
131	How to Audit ERP I	<p>Andy Cataldo, CISA <i>Technology Audit Manager</i> Estee Lauder Companies, Inc.</p> <p>Janak Master Estee Lauder Companies, Inc.</p> <p>Lorraine Peoples, CISA <i>Vice President—Internal Control Department</i> Estee Lauder Companies, Inc.</p>	<ul style="list-style-type: none"> • Recognize challenges to the audit process • Identify the significance of master data and configurable controls • Identify the significance of security controls • Understand key risks associated with auditing ERP systems • Prepare and execute an integrated audit of ERP systems
211	CoBIT Frameworks B	Donald Caniglia, CISA, CISM, CGEIT <i>Senior Associate</i> Jon Campbell & Associates	<ul style="list-style-type: none"> • Identify how CoBIT supports the characteristics of a control framework • Understand the premise of the CoBIT framework • Identify the components and functions of the CoBIT framework • Identify the role of CoBIT IT processes and the four IT domains • Understand IT resources and information criteria
221	CoBIT—Application Controls B	Donald Caniglia, CISA, CISM, CGEIT <i>Senior Associate</i> Jon Campbell & Associates	<ul style="list-style-type: none"> • Describe the role of CoBIT control objectives and control practices • Identify the tools that the CoBIT framework provides as part of the management guidelines • Understand how these tools are applied for an example process—PO10 • Describe the role of the <i>Assurance Guide</i>

Track 1—IT Audit Core Competencies

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
231	How to Audit Active Directory—A Basic Review B	Barry Lewis, CISM, CGEIT <i>President</i> Cerberus ISC Inc.	<ul style="list-style-type: none"> • Know what directory services are and how they are used • Understand key concepts and protocols used in directory services • Understand how Active Directory facilitates security in your business • Identify the critical components and how they relate to one another • Comprehend auditing guidelines to obtain information on where to focus your security assessment • Know how you can manage risk using Active Directory
241	Audit and Control of Windows 2008 I	Barry Lewis, CISM, CGEIT <i>President</i> Cerberus ISC Inc.	<ul style="list-style-type: none"> • Understand the key security functions in Windows 2008 • Identify and understand the risks involved • Implement an effective step-by-step audit • Choose the appropriate control practices
311	Auditing Your UNIX and Linux Operating System I	Michael Schiller, CISA <i>IT Manager</i> Texas Instruments	<ul style="list-style-type: none"> • Know how to audit UNIX and Linux systems • Identify specific audit steps • Discuss the risks being addressed • Identify tools and resources for enhancing your UNIX and Linux audits
321	Data Analytics I	David Chiang <i>General Manager and Director, Professional Services</i> ACL Services Ltd.	<ul style="list-style-type: none"> • Understand the challenges of performing data analytics and how to overcome them • Recognize the data analytical tools in use today, along with the pros and cons of each • Recognize the difference between continuous monitoring and continuous auditing and how they differ • Ascertain what knowledge resources are available through the support groups associated with the tools • Learn from examples of frauds that have been uncovered using data analytical tools and tools specific to the practice of cyber forensics • Identify sources of training and knowledge for specific tools such as ACL and IDEA
331	System Development Life Cycle and Change Management B	Paul Hoshall, CISA <i>Principal</i> Hoshall and Associates	<ul style="list-style-type: none"> • Recognize common risks and problems in systems development • Identify causes and potential solutions of these risks and problems • Ascertain alternative system development audit methods, including benefits and drawbacks • Determine alternatives and guidelines on auditing systems development
411	How to Audit Networks I	Harshul Joshi, CISA, CISM, CGEIT <i>Director, Information Technology Services</i> CBIZ	<ul style="list-style-type: none"> • Understand auditing perimeter devices • Recognize network segmentation • Detect threat and vulnerabilities at the network layer • Comprehend escalation matrix and mitigation controls
421	How to Audit Databases—Where to Start and What to Avoid I	Nam Wu <i>Database Security Engineer</i> Qualys	<ul style="list-style-type: none"> • Identify the key components of a database and where auditing should occur • Understand how to audit databases for security configurations and hardening options • Understand the components of a database and how they impact risk and business continuity • Understand the pitfalls and lessons learned, and how to avoid them during an audit cycle for databases • Measure successful customer implementations through best practices

Track 2—IT Audit Tools and Competencies

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
112	A Risk-based Approach to Segregation of Duties I	Michael J. Adolphson, CISA, CISM <i>Senior Manager</i> Ernst & Young, LLP Justin T. Greis, CISA, CISM, CGEIT <i>Manager</i> Ernst & Young, LLP	<ul style="list-style-type: none"> Understand the underlying concepts behind segregating duties within an application and across applications Understand segregation of duties (SoD) terminology, its impact on the organization, and how to define SoD risk thresholds Understand the risk based approach and critical success factors for testing SoD, regardless of application or platform Identify and understand SoD mitigation and remediation techniques Discuss internal audit's role in SoD compliance. Discuss how companies can work effectively with external audit to achieve compliance
122	Latest Hacker Threats and How to Counter Them I	David Rhoades <i>Senior Consultant</i> Maven Security Consulting Inc.	<ul style="list-style-type: none"> Understand recent developments in hacker tools and techniques and how these developments impact you Discuss emerging trends in cybercrime and legislation Identify defensive and preventative countermeasures to implement Use self-audit techniques Discuss security issues from a wide variety of technologies, including VoIP, wireless, web 2.0, DNS, and 0-day topics
132	How to Understand Continuous Monitoring and Auditing—Tools Specific A	Pradeep Bhandari <i>IT Controls Analyst</i> Huntington Bank Joe Dupree, CISA <i>Unit Leader, Market Development</i> Infogix Inc.	<ul style="list-style-type: none"> Define business challenges associated with unchecked and antiquated auditing processes Formulate strategies in planning and implementing automated information controls Help drive down auditing and compliance costs Assess the array of automated control types to consider and identify the controls that best suit your business needs
212	How to Audit SAP A	Thomas Donohue, CISA <i>Manager</i> Deloitte & Touche Michael Juergens, CISA, CGEIT <i>Principal</i> Deloitte & Touche	<ul style="list-style-type: none"> Recognize the fundamental concepts of auditing SAP security including key risks related to access to programs and data Know how SAP-specific functionality impacts the way security audits are performed Identify the functionality of SAP basis security, the specific risks and potential controls, and suggested audit steps Understand security considerations for change management, organization and management, roles and profiles, security inheritance and system parameters Gather process information, identify risks, evaluate control design, and validate operating effectiveness for SAP-specific security functions Consider the sensitive access and segregation of duties risks within SAP Articulate SAP security issues to management/clients and explain the impact
232	How to Audit Oracle Applications I	Vanessa Vacca Deloitte	<ul style="list-style-type: none"> Identify Oracle audit tools and techniques Understand related audit and security issues in an Oracle database management system Learn practical approaches for evaluating and implementing database security and control

Track 2—IT Audit Tools and Competencies

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
312	Mobile Application Security I	Eugene Schultz, CISM (Honorary) <i>Chief Technology Officer</i> Emagined Security	<ul style="list-style-type: none"> Describe the basics of mobile computing functionality Describe vulnerabilities in mobile computing environments (including vulnerabilities in applications for handheld devices) and the seriousness of each Explain the major types of controls that can be used to mitigate risk in mobile computing environments and cost-benefit ratios associated with each Explain major audit issues relevant to mobile computing environments
322	The Impact of Social Networking on the IT Audit Universe B	Charlie Blanchard, CISA, CISM Deloitte & Touche LLP	<ul style="list-style-type: none"> Identify how social networking sites have evolved from ways to reconnect with old friends to competitive tools used by organizations to market their products Discover how this tool allows auditors to reach out to other audit professionals and to respond with "how to" requests Understand why social networks like LinkedIn and Facebook provide amazingly wide visibility, and why that is the good and the bad news Utilize tools like LinkedIn in job searches for both recruiters and employers to find not just qualified, but candidates that are strongly recommended Establish virtual customer focus groups, which allow enterprises to solicit innovative ideas from visitors and comments from customers Develop marketing programs issued to those who actively visit your enterprises
332	Cloud Computing—An Auditor's Perspective I	Jill Farrington <i>Partner</i> KPMG LLP Sailesh Gadia, CISA <i>Manager</i> KPMG LLP	<ul style="list-style-type: none"> Understand the emerging importance of cloud computing and recognize the associated increase in risk exposure Scope and conduct a risk-based audit of cloud computing environments in accordance with ISACA guidance/frameworks including COBIT Analyze authentication and access control mechanisms in cloud computing environments Utilize tools and techniques relevant to cloud computing to conduct an audit of a cloud computing environment and produce an audit report
412	How to Advise and Audit Your Organization's Business Continuity and Disaster Recovery Plans I	Michael A. Berardi, Jr., CISA, CGEIT <i>Senior Audit Manager</i> Nestlé	<ul style="list-style-type: none"> Learn the critical components of disaster recovery (DR) and business continuity (BC) plans and why they are often forgotten Obtain an understanding of the differences and interdependencies between BC and DR Determine the prevailing software tools for creating and maintaining BC and DR plans Identify the group within the organization responsible for BC and DR plans, and the advantages and disadvantages of various reporting relationships Understand the advantages and disadvantages of the prevalent software Assess the need for a business impact assessment
422	An Interdisciplinary Approach to Audit Effectiveness I	Brian Barnier, CGEIT <i>Principal</i> ValueBridge Advisors	<ul style="list-style-type: none"> Collaborate with resources from other areas of the organization Help auditors address practical needs, such as: overcome reduced audit resources in the face of greater assurance needs and build subject matter expertise in the areas being auditing Learn approaches to working with other disciplines to build the knowledge and resource team Learn how to incorporate and leverage re-engineered business processes, shared services, and processes impacted by merger, acquisition or divestiture

Track 3—Techniques for Evaluating Business Practices and Professional Development

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
113	How to Break the Auditor and Security Manager Stereotype A	Wendy Goucher <i>Security Empowerment Consultant</i> Idrach Ltd.	<ul style="list-style-type: none"> • Understand the role of stereotypes in business communication in general • Recognize how perceptions and prejudices can affect the effectiveness of policies and procedure • Analyze the stereotypical traits and consider which need to be encouraged, and which lost • Demonstrate insight into how an unhelpful image can be changed • Recognize the benefits that image change can bring
123	Building and Maintaining Influential Relationships I	Michael A. Berardi, Jr., CISA, CGEIT <i>Senior Audit Manager</i> Nestlé Mark Phillips, CISA <i>IT Audit Director</i> Duke University and Duke Medicine	<ul style="list-style-type: none"> • “Meet and Greet”—gain an understanding of the components of the organization, the key players and their roles, hot topics and politics • Earn respect—start small and focus on quick wins • Focus on the business first, IT second • Identify the keys to cultural tolerance for change • Work within cultural tolerance for change • Effect enhancements to the management of risk and incorporation of controls • Recognize techniques for communicating technical information to executive management • Detect sources of support for your message and increasing the tolerance for change • Know the advantages of integrating external resources into your internal risk and controls testing • Appreciate the challenges of for-profits vs. not-for-profit organizations • Learn the best practices for effecting change in the management of risks and controls
133	Generational Issues I	Caitlin McGaw <i>Regional Director of Recruitment</i> Lander International, LLC	<ul style="list-style-type: none"> • Understand why there is a need to be aware of generational issues • Understand how audit departments can create better value today and tomorrow • Recognize generational differences and the value they each bring to the organization • Appreciate how each generation views career goals • Learn what the future talent pool holds for you and for your enterprise
213	Free Tools—What’s Out There? B	David Hansen, CISA RSM McGladrey	<ul style="list-style-type: none"> • Understand what is available for free use • Conduct a search for free tools • Recognize how to use free tools
223	Know Your Personality and Your Company Culture B	Todd Fitzgerald, CISA, CISM, CGEIT <i>Senior Technical Compliance Advisor</i> National Government Services	<ul style="list-style-type: none"> • Become self-aware of your personality type using multiple psychological methods • Increase communication capability with others by knowing their communication style • Evaluate your own company culture to determine how to sell initiatives • Enhance personal organizational effectiveness • Get better results by understanding what makes people behave the way they do

Track 3—Techniques for Evaluating Business Practices and Professional Development

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
233	<p>Providing Assurance on Systems and the Integrity of Information Using the AICPA Framework</p> <p>B</p>	<p>Chris Halterman Executive Director Advisory Services Chair AICPA Trust Data Integrity Task Force Ernst & Young</p>	<ul style="list-style-type: none"> Understand how to provide assurance on the integrity of information and the reliability of systems utilizing the Trust Services Principles and Criteria Understand the AICPA Assurance Services Executive Committee initiatives on the assurance on systems Review the changes made to the Trust Services Principles and Criteria for the reliability of systems Provide an overview of the new measurement criteria currently under development to provide assurance the integrity of information Learn what practitioner guidance content is being drafted for the application of the Proposed SSAE, Reporting on Controls at a Service Organization, to nonfinancial systems using the Trust Services Principle and Criteria and what it may mean to your organization
243	<p>How to Work with Boards and Other Stakeholders: A Primer for New IT Managers</p> <p>I</p>	<p>An Advanced Panel</p>	<ul style="list-style-type: none"> Understand the importance of meeting and building relationships with both stakeholders and the Audit Committee Recognize the importance of explaining technical concepts and issues using business terminology Recognize and realize the critical importance of getting to know and building relationships with The Board and key stakeholders Utilize web tools such Google and social networks to learn about The Board and key Stakeholders before you even meet them Discern when and in what forums communication on critical or sensitive topics take place
313	<p>Developing an Information Risk Management and Security Strategy</p> <p>A</p>	<p>John P. Pironti, CISA, CISM, CGEIT Chief Information Risk Strategist Archer Technologies</p>	<ul style="list-style-type: none"> Understand the key concepts and considerations that should be evaluated when developing an information risk management and security strategy Identify the current leading practices and concepts in strategy design and development Identify whether or not the strategy that is being developed and implemented is appropriate and effective for an organization Spot common mistakes and oversights that are made by organizations when they develop an information risk management and security strategy Know which key elements to include in strategy development Develop methods and practices for developing, testing and evaluating strategy Learn through case studies that describe how organizations have successfully and unsuccessfully approached strategy development and implementation
323	<p>How to Close the Gap Between Information Security and Audit</p> <p>I</p>	<p>Eugene Schultz, CISM (Honorary) Chief Technology Officer Emagined Security</p> <p>John Tannahill, CISM, CGEIT Management Consultant J. Tannahill & Associates</p>	<ul style="list-style-type: none"> Describe the types of gaps that frequently exist between the audit and information security functions within organizations Describe areas and issues about which auditors and information security professionals typically have different views and approaches and why Describe weaknesses and shortcomings common to both the audit and information security areas and how they can be overcome Explain and evaluate potential approaches to closing the gap between these functions
333	<p>Organizational and Individual Ethics—Value Added Audit</p> <p>I</p>	<p>Graham Murphy Mid West Practice Leader KPMG Forensic</p> <p>Peter Bradford Director KPMG LLP</p>	<ul style="list-style-type: none"> Assess an IT audit program as it may relate to ethics and compliance Understand the key elements of an effective ethics program Recognize typical fraud and misconduct risks that can potentially undermine company business objectives Understand how to improve efforts to combat the risks of fraud and misconduct Strengthen corporate governance programs and help reduce/manage reputational risks

Track 3—Techniques for Evaluating Business Practices and Professional Development

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
413	How to Use Professional Credentialing for Career Development B	Caitlin McGaw <i>Regional Director of Recruitment</i> Lander International LLC	<ul style="list-style-type: none"> Utilize ongoing survey results that discuss why certification is gaining global appeal in the profession Understand what the Certified in the Governance of Enterprise IT® (CGEIT®) certification means for Senior Management in working towards continuous monitoring for constant vigilance Develop a career-path road map for professional development using certification programs in the security profession Use mentoring and coaching programs to implement the road map Understand the value certification brings to the organization Know the future plans for the certification programs
423	How to Make SAS 70 Work for You I	Michael Dean, CISA <i>Manager, IT Audit</i> Clifton Gunderson, LLP	<ul style="list-style-type: none"> Understand situations in which SAS 70 audits are appropriate or not appropriate Understand the kind of assurance SAS 70 audits provide Write control descriptions to satisfy stated control objectives Gather and assess evidence Appropriately manage an SAS 70 audit

Track 4—Emerging Issues and ISACA Research

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
114	How to Construct a Dashboard—A Case Study I	Francisco Seixas Neto, CISA, CGEIT <i>Partner</i> EGV Consultoria	<ul style="list-style-type: none"> Discuss some IT management metrics Understand how to create a IT governance dashboard view through a balanced scorecard (BSC) hierarchical structure of metrics and indicators Understand how to use the cause and effect relationship shown in the dashboard to promote improvements in IT environment Recognize how to use CoBIT and its components to initiate and support the BSC dashboard creation Discuss an IT governance dashboard implementation strategy based in the indicators management
124	How to Achieve Security Governance: Working with Management, Control Frameworks and Auditors I	Todd Fitzgerald, CISA, CISM, CGEIT <i>Senior Technical Compliance Advisor</i> National Government Services	<ul style="list-style-type: none"> Differentiate between control standards, frameworks and regulations Harmonize control standards including CoBIT, PCI, ISO 27000, NIST 800-53 and FISCAM Work effectively with internal and external auditors Examine various security organizational structures Apply an 11-step approach to successful compliance

Track 4—Emerging Issues and ISACA Research

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
214	Building a Sustainable Information Security Risk Management Program Using Six Sigma 	Shawna Flanders, CISA, CISM <i>Productivity Specialist</i> PS CU-FS Process Innovation & Excellence	<ul style="list-style-type: none"> • Understand Six Sigma • Understand how the Six Sigma methodology may be used in a security risk management program • Identify the steps to building a sustainable program • Recognize how various standards impact the program • Monitor the program to keep it current
224	A Risk IT Framework Implementation Case Study 	Francisco Seixas Neto, CISA, CGEIT <i>Partner</i> EGV Consultoria	<ul style="list-style-type: none"> • Understand the Risk IT Framework to promote improvements in the risk management process • Recognize how to evolve from the actual internal control management process to a risk management process • Discover how to use CoBIT components to achieve a qualitative way to determine risk with a business focus
234	Operational Excellence— A Case Study in the Practical Integration of CoBIT and ITIL 	Marlin Ness, CGEIT <i>Executive Director</i> Ernst & Young, LLP Dan Stavola <i>Senior Manager</i> Ernst & Young, LLP	<ul style="list-style-type: none"> • Understand CoBIT 4.1 and ITIL IT service management and implement the two frameworks into production • Discuss CoBIT 4.1 control objectives • Understand ITIL IT service management assessments and implementations • Assess, analyze, design, implement, and integrate frameworks • Recognize a pragmatic approach to leveraging leading practices and methods, and the harmonization of standards
244	How to Manage Segregation of Duties in an SAP Environment 	Prateek Jain, CISA <i>Senior</i> Ernst & Young	<ul style="list-style-type: none"> • Understand the basic SAP security concept • Explain the SoD concept • Analyze the SAP Security Complexity and how the SoD tools help manage SoD issues • Assess SoD using SAP GRC business solutions
314	Continuous Monitoring and Metrics in an SAP Environment 	Sunita Suryanarayan Deloitte & Touche	<ul style="list-style-type: none"> • Understand the challenges with deploying a continuous monitoring solution is how to make it practical • Recognize steps to develop a pragmatic approach to continuous monitoring • Learn what approaches and tool sets are required • Identify the specific items to monitor • Discover practical approaches for identifying those exceptions that are meaningful • Determine sustainability • Identify and measure your return on investment
324	Using CoBIT to Align Internal IT Controls With an Outsourcer's Control Framework 	William L. Wayland, CISA <i>Risk Advisory Services Professional</i> Jefferson Wells International	<ul style="list-style-type: none"> • Explain key risks inherent the basic types of outsourcing • Recognize the difference between contractors and outsourcers • Assess the risks of applying your controls to an outsourcer • Describe which CoBIT objectives fit well with each type of outsourcing • Describe what an ISO 27001 certification represents from a control standpoint • How to cross-reference CoBIT 4.1, ISO 27001, and company control objectives and policies • How to develop a risk-based matrix to support consistent control objectives for multiple types of outsourcers

Track 4—Emerging Issues and ISACA Research

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
334	European Network and Information Security Agency I	ENISA Representative	<ul style="list-style-type: none"> • Understand this body of expertise, set up by the European Union (EU), and the objective to enhance the capability of the EU, the EU Member States and the business community • Understand how ENISA research helps the audit and security community to prevent, address and respond to network and information security problems, and to carry out specific technical, scientific tasks in information security • Recognize how The Agency also assists the European Commission in the technical preparatory work for updating and developing community legislation in network and information security • Identify how The Agency's Mission is essential to achieve a high and effective level of network and information security within the EU
414	Vendors and Privacy—What Companies Can do to Minimize Their Risk I	A Panel Discussion Moderator: Gregory Hedges, CISM <i>Managing Director</i> Protiviti Panelists: John Bingham, CISA, CISM <i>Chief Privacy Officer</i> Whirlpool Corp. Michael Brauneis <i>Director</i> Protiviti Andrew Retrum, CISA <i>Associate Director</i> Protiviti Thomas Smedinghoff <i>Partner</i> Wildman Harrold	<ul style="list-style-type: none"> • Discuss different approaches and techniques to prioritizing privacy risks for company vendors • Understand the significance and shortcomings of privacy-related contractual obligations • Outline specific, repeatable steps that can be taken to assess vendor privacy risks • Understand the impact the struggling economy has on vendor relationships • Take actionable steps to reduce vendor privacy risks over time • Address a vendor privacy breach
424	Enterprise Data Management I	Michael A. Berardi, Jr., CISA, CGEIT <i>Senior Audit Manager</i> Nestlé	<ul style="list-style-type: none"> • Recognize the significant risk factors and control considerations that organizations face each day • Detect qualitative and quantitative levels of justification for data management as a full-time commitment from creation through destruction • Identify the ten most critical requirements to be defined for managing your data • Ascertain critical considerations and creating data classifications • Understand the content of data or data about data, commonly known as Metadata • Know regulatory requirements such as eDiscovery and renewed importance of data availability • Identify security and environmental data concerns beyond the data center walls • Spot modern myths and legends—insecurity through obscurity, do you know where your sensitive data is hiding?

Track 5—IT Governance and Compliance

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
115	Fraud—How the IT Auditor Can Help in Managing Fraud Risk I	Jeffrey M. Krull, CISA <i>Senior Manager</i> PricewaterhouseCoopers	<ul style="list-style-type: none"> Define fraud and recognize some common examples and scenarios for fraud Understand strategies for helping to detect and investigate a fraud Recognize weaknesses in the IT controls that allow a fraud to occur Learn some common scenarios and strategies for helping to identify potential fraud
125	SAP—GRC Tools and Dashboards I	<p>Matt Burback <i>Manager Projects, H-D Information Services</i> Harley-Davidson Motor Company</p> <p>Tim Van Ryzin, CISA, CISM <i>IT Audit Manager</i> Harley-Davidson Motor Company</p> <p>Cameron Yazdani, CISA <i>Manager, IT Audit</i> Briggs & Stratton</p>	<ul style="list-style-type: none"> Plan and execute a SAP GRC implementation Implement GRC process controls for business process auditing and control self assessment management; use GRC access controls for user access and segregation of duties testing, GRC Fire Fighter for super-user access controls; and GRC Role Expert for user profile design Recognize through a highly interactive exchange which SAP GRC topic areas are critical to the enterprise
215	Cloud Computing I	Marne E. Gordan <i>Regulatory Analyst,</i> <i>Corporate Security Strategy</i> IBM	<ul style="list-style-type: none"> Identify the three major types of cloud deployments, and the pros and cons of each Understand security and compliance risks associated with the three major types of cloud deployments Adapt PCI, HIPAA, SOX 404, and state security and privacy requirements to address cloud computing Implement the top five measures each organization must take in order to appropriately address cloud security for a positive compliance outcome
225	How to Take the Complexity out of Compliance Through Better Integration I	Nick Nikols <i>Vice President</i> <i>Identity and Security</i> Novell	<ul style="list-style-type: none"> Reduce redundancies and cut costs by automating and enforcing common controls across disparate systems, including SAP Map IT controls to business owners to reduce risk exposure Integrate the various sets of roles, entitlements, and policies across the enterprise ecosystem Create a future-focused IT governance and compliance program that enhances your security posture by aligning tactical IT processes and controls to business objectives
235	Contracting for Security in the Cloud: Creating and Auditing the Essential Security Control I	Jeffrey Ritter <i>Chief Executive Officer</i> Waters Edge	<ul style="list-style-type: none"> Define the contract that regulates the relationship between the parties Understand the security, business and legal rules that must be navigated Identify the key strategies to identify and organize the rules to create and audit cloud services agreements, based on the work of the Cloud Security Alliance Achieve the objectives for effective information security between the parties Assure that everyone's security duties are properly created and capable of enforcement

Track 5—IT Governance and Compliance

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
245	<p>Two Roads Diverged—Security vs. Compliance</p> <p>I</p>	<p>Marne E. Gordan Regulatory Analyst, Corporate Security Strategy IBM</p>	<ul style="list-style-type: none"> • Understand the security principles behind the prevalent information security regulations and standards • Identify commonalities between multiple security regulations and standards • Adapt current control mechanisms to satisfy multiple audit and compliance reporting requirements • Identify the eight foundation control areas that are key to a successful security posture • Implement an effective information security program from which compliance is a natural by-product
315	<p>How the IT Auditor Can Stay Relevant and Communicate Effectively</p> <p>A</p>	<p>Michael Siwicki, CISA Senior Manager PricewaterhouseCoopers LLP</p>	<ul style="list-style-type: none"> • Broaden the message of your audit plan and findings to the entire executive management team and board of directors • Train IT auditors to help communicate their messaging to broaden their relevance throughout an organization to outside of an IT Environment • Learn through solid examples of how this has worked to build a more enhanced brand of IT auditor at a wide range of companies facing a multitude of risks and challenges
325	<p>Auditing IT Governance: A Multiphased Approach</p> <p>I</p>	<p>Lance Turcato, CISA, CISM, CGEIT Deputy City Auditor— IT Audit Division City of Phoenix, City Auditor Department</p>	<ul style="list-style-type: none"> • Develop a multi-phased IT governance audit strategy and plan by leveraging the key components of an effective IT governance structure/framework • Develop audit plans for assessing specific components of the organization's IT governance structure, policies and standard operating procedures • Design effective audit testing plans to evaluate the effectiveness of the organization's IT governance practices • Cultivate effective governance mechanisms for measuring IT performance, resource management, risk mitigation, and achievement of business objectives and expectations for IT • Ensure comprehensive and effective audit coverage by leveraging industry standards for IT governance such as COBIT 4.1, Val IT, and ISO/IEC-38500 (Corporate Governance of IT)
415	<p>How to Turbo Charge Your IT Compliance Program</p> <p>I</p>	<p>Michael Bargeruff Director, IT Compliance & e-Discovery Apollo Group Inc.</p>	<ul style="list-style-type: none"> • Gain insight and knowledge to implement new methods and approaches to handle the increasing demands of compliance obligations with increased efficiency and transparency • Understand how others in the enterprise view IT compliance • Identify how to establish partnerships, alliances and buy-in, all while minimizing overhead associated with tracking and reporting IT compliance progress • Build partnerships between IT compliance personnel and internal audit staff
425	<p>In Defense of Compliance</p> <p>I</p>	<p>Rex Booth Senior Manager Grant Thornton</p> <p>Kenneth Newman, CISM Vice President and Information Security Manager Central Pacific Bank</p>	<ul style="list-style-type: none"> • Understand the barriers to compliance and how to overcome them • Recognize why compliance is viewed differently by various stakeholders • Understand the needs of different stakeholders • Understand why compliance and security only appear to be competing goals • Appreciate how and why compliance and security can work together • Know the values of embracing compliance vs. the risks of failing to do so • Effectively communicate to help bridge the compliance gap • Apply these principles to personal career goals

Preconference Workshops		CONFERENCE TRACKS		Monday 19 April 2010				Tuesday 20 April 2010	
Saturday 17 April 2010	Sunday 18 April 2010			8:30 a.m.– 10:00 a.m.	10:30 a.m.–12 Noon	1:30 p.m.–3:00 p.m.	3:30 p.m.–5:00 p.m.	8:30 a.m.–10:00 a.m.	10:30 a.m.–12 Noon
WS1 CISA Review Weekend I David Baker, Aaron Parks, CISA, CISM, Ken Schmidt, CISA and Paul Phillips, CISA, CISM		Track 1 IT Audit Core Competencies		111 IT Security Control Frameworks and Standards Overview B Todd Fitzgerald, CISA, CISM, CGEIT	121 IT Audit Fundamentals I Andy Cataldo, CISA, Janak Master and Lorraine Peoples, CISA	131 How to Audit ERP I Andy Cataldo, CISA, Janak Master and Lorraine Peoples, CISA	211 CobIT Frameworks B Donald Caniglia, CISA, CISM, CGEIT	221 CobIT—Application Controls B Donald Caniglia, CISA, CISM, CGEIT	
		Track 2 IT Audit Tools and Competencies		112 A Risk-based Approach to Segregation of Duties I Michael J. Adolphson, CISA, CISM and Justin T. Greis, CISA, CISM, CGEIT	122 Latest Hacker Threats and How to Counter Them I David Rhoades	132 How to Understand Continuous Monitoring and Auditing—Tools Specific A Pradeep Bhandari and Joe Dupree, CISA	212 How to Audit SAP A Thomas Donohue, CISA and Michael Juergens, CISA, CGEIT		
WS2 Remote Security Testing for Web Applications—Demonstration Based I David Rhoades		Track 3 Techniques for Evaluating Business Practices and Professional Development		113 How to Break the Auditor and Security Manager Stereotype A Wendy Goucher	123 Building and Maintaining Influential Relationships I Michael A. Berardi Jr., CISA, CGEIT and Mark Phillips, CISA	133 Generational Issues I Caitlin McGaw	213 Free Tools—What's Out There? B David Hansen, CISA	223 Know Your Personality and Your Company Culture B Todd Fitzgerald, CISA, CISM, CGEIT	
		Track 4 Emerging Issues and ISACA Research		114 How to Construct a Dashboard—A Case Study I Francisco Seixas Neto, CISA, CGEIT	124 How to Achieve Security Governance: Working with Management, Control Frameworks and Auditors I Todd Fitzgerald, CISA, CISM, CGEIT		214 Building a Sustainable Information Security Risk Management Program Using Six Sigma I Shawna Flanders, CISA, CISM	224 A Risk IT Framework Implementation Case Study I Francisco Seixas Neto, CISA, CGEIT	
WS3 Risk IT Management I Brian Barnier, CGEIT, and Urs Fischer, CISA		Track 5 IT Governance and Compliance		115 Fraud—How the IT Auditor Can Help in Managing Fraud Risk I Jeffrey M. Krull, CISA	125 SAP—GRC Tools and Dashboards I Matt Burback, Tim Van Ryzin, CISA, CISM and Cameron Yazdani, CISA		215 Cloud Computing I Marne E. Gordan	225 How to Take the Complexity Out of Compliance Through Better Integration I Nick Nikols	
		Track 6 Information Technology Security and Data Protection		116 Advanced Threats: How to Fight Cybercrime A Edward Schwartz, CISA, CISM	126 Web and XML Threats and Mitigation I Steve Orrin		216 How to Keep Your Company Out of the Headlines—Data Loss Prevention B David Chan, Chris Kostick, Tushar Padhiar, CISA, CISM	226 From Virtualization vs. Security to Virtualization-based Security I Steve Orrin	
WS4 How to Audit and Secure Microsoft SQL Server I John Tannahill, CISA, CGEIT	WS5 Using CobIT in Audit and Assurance I Donald Caniglia, CISA, CISM, CGEIT	Track 7 IT Risk and Exposure Management		117 How to Develop and Audit the IT Risk Management Function I Brian Barnier, CGEIT, Michael A. Berardi Jr., CISA, CGEIT and Robert Johnson, CISA, CISM, CGEIT		127 IT Security vs. Information Security I Owen Watkins	217 How to Analyze the Risks of Outsourcing and Offshoring I Harshul Joshi, CISA, CISM, CGEIT and Lorraine Peoples, CISA	227 Establishing Effective ERM IT: Implementation and Operational Issues of the New Risk IT Framework I Urs Fischer, CISA	

Keynote Address

		Wednesday 21 April 2010				Thursday 22 April 2010		Friday 23 April 2010				
1:30 p.m.-3:00 p.m.	3:30 p.m.-5:00 p.m.	8:30 a.m.-10:00 a.m.	10:00 a.m.-1:30 p.m.	1:30 p.m.-3:00 p.m.	3:30 p.m.-5:00 p.m.	8:30 a.m.-10:00 a.m.	10:30 a.m.-12 Noon	1:30 p.m.-5:00 p.m.	9:00 a.m.-12:30 p.m.			
231 How to Audit Active Directory—A Basic Review B Barry Lewis, CISM, CGEIT	241 Audit and Control of Windows 2008 I Barry Lewis, CISM, CGEIT	311 Auditing Your UNIX and Linux Operating System I Michael Schiller, CISA	Exhibits	321 Data Analytics I David Chiang	331 SDLC/Change Management B Paul Hoshall, CISA	411 How to Audit Networks I Harshul Joshi, CISA, CISM, CGEIT	421 How to Audit Databases—Where to Start and What to Avoid I Nam Wu	WS6 IT Controls Monitoring I Michael Garber, CGEIT and Kenneth Vander Wal, CISA				
232 How to Audit Oracle Applications I Vanessa Vacca	312 Mobile Application Security I Eugene Schultz, CISM (Honorary)	322 The Impact of Social Networking on the IT Audit Universe B Charlie Blanchard, CISA, CISM		332 Cloud Computing—An Auditor's Perspective I Jill Farrington and Sailesh Gadia, CISA	412 How to Advise and Audit on BC and DR Plans I Michael A. Berardi Jr., CISA, CGEIT	422 An Interdisciplinary Approach to Audit Effectiveness I Brian Barnier, CGEIT	WS7 Security and Audit of Oracle in Today's Enterprise I John Tannahill, CISM, CGEIT					
233 Providing Assurance on Systems and the Integrity of Information Using the AICPA Framework B Chris Halterman	243 How to Work with Boards and Other Stakeholders: A Primer for New IT Managers I An Advanced Panel	313 Developing an Information Risk Management and Security Strategy A John P. Pironti, CISA, CISM, CGEIT		323 How to Close the Gap Between Information Security and Audit I Eugene Schultz, CISM (Honorary) and John Tannahill, CISM, CGEIT	333 Organizational and Individual Ethics—Value Added Audit I Graham Murphy and Peter Bradford	413 How to Use Professional Credentialing for Career Development B Caitlin McGaw			423 How to Make SAS 70 Work for You I Michael Dean, CISA			
234 Operational Excellence—A Case Study in the Practical Integration of COBIT and ITIL I Marlin Ness, CGEIT, and Dan Stavola	244 How to Manage Segregation of Duties in an SAP Environment I Prateek Jain, CISA	314 Continuous Monitoring and Metrics in an SAP Environment I Sunita Suryanarayan		324 Using COBIT to Align Internal IT Controls With an Outsourcer's Control Framework I William L. Wayland, CISA	334 European Network and Information Security Agency I ENISA	414 Vendors and Privacy—What Companies Can do to Minimize Their Risk I A Panel Discussion			424 Enterprise Data Management I Michael A. Berardi Jr., CISA, CGEIT			
235 Contracting for Security in the Cloud: Creating and Auditing the Essential Security Control I Jeffrey Ritter	245 Two Roads Diverged—Security vs. Compliance I Mame E. Gordan	315 How the IT Auditor Can Stay Relevant and Communicate Effectively A Michael Siwicki, CISA		325 Auditing IT Governance: A Multiphased Approach I Lance Turcato, CISA, CISM, CGEIT	415 How to Turbo Charge Your IT Compliance Program I Michael Bargerhuff	425 In Defense of Compliance I Rex Booth and Kenneth Newman, CISM			WS8 GRC: Managing the Corporate IT Portfolio I Al Marcella Jr., CISA			
236 Windows 7 Security—An Audit Perspective I John Tannahill, CISM, CGEIT	246 Threat and Vulnerability Analysis A John P. Pironti, CISA, CISM, CGEIT	316 ERP Security and Oracle Security I Jeffrey M. Krull, CISA		326 How to Implement Security Controls for PCI I Harshul Joshi, CISA, CISM, CGEIT	416 Seven Things Hackers Don't Want You to Know About PCI I Bruce Sussman, CISA	426 Electronic Medical Record Privacy and Security B Sagi Leizerov				WS9 Harmonizing Standards—Achieving Compliance With Security Regulations I Todd Fitzgerald, CISA, CISM, CGEIT		
237 Leveraging Technology for Effective Risk Management I Sarah Adams, CISA, Lorraine Peoples, CISA and Robert Zanella, CISA	317 How to Manage Network Risk I Robert Johnson, CISA, CISM, CGEIT	327 A Case Study on Crisis Management I Edward Minyard		417 IT Internal Audit Risk Assessment I Sarah Adams, CISA and Kay Lynn Parks, CISA	427 How to Assess Cost-Cutting Risks to the Organization A Michael Juergens, CISA, CGEIT							

Track 6—IT Security and Data Protection

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
116	Advanced Threats: How to Fight Cybercrime A	Edward Schwartz, CISA, CISM <i>Chief Security Officer</i> NetWitness Corp.	<ul style="list-style-type: none"> • Understand how “status quo” thinking has caused a dangerous precedent in the perceived security of an organization • Know how the criminal underground has developed into a “virtual swap meet” for exploit techniques, botnets, malware and identities • Recognize how current malicious code technologies and exploitation techniques are bypassing existing security controls • Build an internal team that is tailored for advanced threat research • Use threat feeds and research blacklists to analyze malware and malicious code • Describe why an advanced threat management capability can focus remediation efforts where they are needed most
126	Web and XML Threats and Mitigation I	Steve Orrin <i>Director of Security Solutions</i> Intel Corp.	<ul style="list-style-type: none"> • Present the threat models and classifications for Web and XML risks • Identify the root causes of many of the application layer threats • Demonstrate several common application layer attacks • Manage strategies for effective compliance, risk mitigation and remediation of application layer threats • Weigh the cost vs. benefits of these mitigation strategies • Effectively evaluate tools and practices for auditing and testing security in web and web-services based applications
216	How to Keep Your Company Out of the Headlines—Data Loss Prevention B	David Chan <i>Manager</i> Ernst & Young LLP Chris Kostick <i>Executive Director</i> Ernst & Young LLP Tushar Padhiar, CISA, CISM <i>Senior Manager</i> Ernst & Young LLP	<ul style="list-style-type: none"> • Assess an organization's data loss prevention (DLP) capabilities to help organizations defend against IT security incidents • Articulate the risks of how data loss incidents can result in significant regulatory penalties, legal costs, and brand damage to a company if it is unprepared and does not have a robust incident response program • Define the roles of internal audit and IT in developing and assessing incident response capabilities for protecting, defending and sustaining the organization against data loss incidents • Address common challenges and overcome pitfalls encountered by organizations related to responding to data loss incidents • Complete a sample work program to assess DLP and incident response capabilities • Leverage industry points-of-view and common themes related to data loss prevention and incident response to develop an effective audit approach • Use frameworks and leading practices for reviewing an organization's DLP and incident response capabilities
226	From Virtualization vs. Security to Virtualization-based Security I	Steve Orrin <i>Director of Security Solutions</i> Intel Corp.	<ul style="list-style-type: none"> • Identify platform virtualization mechanisms • Recognize advances in virtualization technologies which improve your security posture • Know and understand strategies for effective compliance and enforcement in virtualized environments • Discuss new ways to secure platforms using virtualization including application isolation and sandboxing, and policy-based execution environments

Track 6—IT Security and Data Protection

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
236	Windows 7 Security— An Audit Perspective I	John Tannahill, CISM, CGEIT <i>Management Consultant</i> J. Tannahill & Associates	<ul style="list-style-type: none"> Understand Windows 7 Security features and mechanisms including Local Security Policy, User Accounts; Action Center; User Access Control, Security Event Logs, Encryption etc. Understand Windows 7 Security in context of the organization and related Windows 2008 Server security including use of GPO Accelerator, Client Security Baselines and Network Access Protection Understand and audit Windows Firewall and advanced security features Secure and audit the Windows 7 operating system environment using security baselines
246	Threat and Vulnerability Analysis A	John P. Pironti, CISA, CISM, CGEIT <i>Chief Information Risk Strategist</i> Archer Technologies	<ul style="list-style-type: none"> Understand the difference between information security and information risk management Describe and give an overview of threat and vulnerability management programs Discuss threat analysis—who, what, when, where and how Explain OSI and OSI methodology Understand vulnerability analysis Discuss risk mitigation strategies Recognize technological options to assist in the operations of the program
316	ERP Security and Oracle Security I	Jeffrey M. Krull, CISA <i>Senior Manager</i> PricewaterhouseCoopers	<ul style="list-style-type: none"> Understand the basic security architecture within Oracle Understand potential strategies for testing Oracle security Prepare IT audit professionals on Oracle security and how Oracle security functions identify potential strategies for effectively testing Oracle security Participate in case study discussions demonstrating the potential magnitude of different security issues
326	How to Implement Security Controls for PCI I	Harshul Joshi, CISA, CISM, CGEIT <i>Director, Information Technology Services</i> CBIZ	<ul style="list-style-type: none"> Understand how to scope the implementation project to build and maintain a secure network Protect data and access control Regulate and manage network vulnerability Monitor and test the network Realize that maintenance is an on-going process and how to sustain a secure network
416	Seven Things Hackers Don't Want You to Know About PCI I	Bruce Sussman, CISA <i>Senior Manager</i> Crowe Horwath LLP	<ul style="list-style-type: none"> Identify seven ways in which sophisticated criminal organizations can bypass the defense of PCI compliant organizations to breach defenses Gain insight into the difference between compliance with a static standard and proactively securing your organization Identify risk mitigation strategies which may be appropriate to your organization Develop strategies to help your organization minimize its exposure, reduce complacency and respond to hackers and their dynamic strategies for penetrating your organization
426	Electronic Medical Record Privacy and Security B	Sagi Leizerov <i>Senior Manager</i> Ernst & Young LLP	<ul style="list-style-type: none"> Understand various privacy and security considerations of implementing and using electronic medical records Discuss the key privacy and security changes to HIPAA in the ARRA regulation Recognize the key challenges to the implementation of electronic medical records from privacy and security perspectives Know what to audit when reviewing the implementation of electronic medical records

Track 7—IT Risk and Exposure Management

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
117	<p>How to Develop and Audit the IT Risk Management Function</p> <p>I</p>	<p>Brian Barnier, CGEIT <i>Principal</i> ValueBridge Advisors</p> <p>Michael A. Berardi, Jr., CISA, CGEIT <i>Senior Audit Manager</i> Nestlé</p> <p>Robert Johnson, CISA, CISM, CGEIT <i>Head of Information and Operations Risk Management</i> ING US Financial Services</p>	<ul style="list-style-type: none"> • Understand IT risk management (IRM) as an emerging function in many organizations and examine its role in today's competitive environment • Learn how this role aligns with lines of defense • learn how to audit the IRM function • Recognize the top 10 risks IRM function covers and why • Comprehend how IRM audit differs from traditional audits • Establish key resources upon which the IRM function is dependent
127	<p>IT Security vs. Information Security</p> <p>I</p>	<p>Owen Watkins <i>Implementation Support Manager, Regional Compliance Office</i> Siemens</p>	<ul style="list-style-type: none"> • Recognize the difference between information security and IT security • Understand the techniques used in its practice, key issues in information security and the nature of current threats • Explain what information security means and its consequences • Discuss topical threats • Discuss pitfalls and successes in current practice
217	<p>How to Analyze the Risks of Outsourcing and Offshoring</p> <p>I</p>	<p>Harshul Joshi, CISA, CISM, CGEIT <i>Director, Information Technology Services</i> CBIZ</p> <p>Lorraine Peoples, CISA <i>Vice President—Internal Control Department</i> Estee Lauder Companies Inc.</p>	<ul style="list-style-type: none"> • Describe a cost-benefit analysis for IT outsourcing • Understand the outsourcing process • Discuss pros and cons of outsourcing and offshoring • Explain risk analysis and compare various options • Discuss the past, present and future of IT outsourcing
227	<p>Establishing Effective Enterprise Risk Management IT: Implementation and Operational Issues of the New Risk IT Framework</p> <p>I</p>	<p>Urs Fischer, CISA</p>	<ul style="list-style-type: none"> • Integrate IT risk management with enterprise risk management (ERM) • Establish and maintain a common risk view and make risk-aware business decisions • Maintain an operational risk profile, and assess and respond to risk • Collect event data, monitor risk, and report exposures and opportunities
237	<p>Leveraging Technology for Effective Risk Management</p> <p>I</p>	<p>Sarah Adams, CISA <i>Director IT Internal Audit</i> Deloitte & Touche LLP</p> <p>Lorraine Peoples, CISA <i>Vice President—Internal Control Department</i> Estee Lauder Companies Inc.</p> <p>Robert Zanella, CISA <i>VP, IT Compliance</i> CA</p>	<ul style="list-style-type: none"> • Understand the current economic climate and how it has made effective risk management a critical business imperative • Identify successful strategies requiring extensive use of IT resources, processes and personnel in order to meet their business objectives • Ascertain how IT can help executives monitor business process execution, and manage risk through comprehensive reporting and assessment • Recognize principles to successfully kick-start the implementation of risk and compliance management • Discover specific techniques used to further mature risk and compliance management functions

Track 7—IT Risk and Exposure Management

SESSION #	SESSION TITLE	PRESENTER	AFTER COMPLETING THIS SESSION, YOU WILL BE ABLE TO:
317	How to Manage Network Risk I	Robert Johnson, CISA, CISM, CGEIT <i>Head of Information and Operations Risk Management</i> ING US Financial Services	<ul style="list-style-type: none"> • Discuss various networks and their complexities • Identify the risks applicable to the network infrastructure • Explain the integration of risk management in the IT infrastructure • Describe controls used to mitigate network risk exposures • Understand the application of industry standards and best practices
327	A Case Study on Crisis Management I	Edward Minyard <i>Partner</i> Accenture	<ul style="list-style-type: none"> • Add a new perspective to your enterprises threat, risk and impact assessments • See firsthand examples of destruction and disruption of major catastrophic disasters including Hurricane Katrina and the recent H1N1 epidemic • Discover new elements to consider during the planning process • Incorporate planning knowledge gained by the “being there” experience
417	IT Internal Audit Risk Assessment I	Sarah Adams, CISA <i>Director IT Internal Audit</i> Deloitte & Touche LLP Kay Lynn Parks, CISA <i>Manager, Internal Audit</i> NRG Energy, Inc.	<ul style="list-style-type: none"> • Understand IT internal audit (IA) risk assessment methodology and risk framework, which provide guidance in conducting IT risk assessments • Develop an understanding of common IT risks in order to be able to perform an IT risk assessment • Learn how to develop an IT risk model and risk universe for your enterprise as part of performing an IT risk assessment • Learn how to develop a risk response, including a risk-intelligent IT internal audit plan based on the risk assessment performed • Learn firsthand based on how an IT risk assessment was performed at NRG Energy, the challenges that were faced and the value it brought to the company
427	How to Assess Cost-Cutting Risks to the Organization A	Michael Juergens, CISA, CGEIT Deloitte & Touche LLP	<ul style="list-style-type: none"> • Identify common cost-cutting activities • Assess common risks around these activities • Determine which cost-cutting activities may hinder more than help • Discuss practical recommendations for reducing risk while achieving cost cutting objectives

Did you know...

ISACA recently developed Risk IT—

A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk. Find out more at www.isaca.org/riskit.

Increase the value of your conference experience and attend one of the pre- and/or postconference workshops. All workshops are one- or two-day events that provide in-depth training on today's hot topics. Preconference workshops will be held Saturday, 17 April 2010 and Sunday, 18 April 2010. One-day preconference workshops will be held Sunday, only. Postconference workshops will be held in two half-day sessions: the afternoon of Thursday, 22 April 2010 and the morning of Friday, 23 April 2010.

Prerequisites for all conference workshops:

Participants should have at least three years of IT experience or equivalent knowledge.

Preconference Workshops

SESSION #	WORKSHOP TITLE	PRESENTER	DESCRIPTION:
WS1	<p>CISA Review Weekend (two-day)</p> <p>I</p> <p>Saturday, 17 April and Sunday, 18 April</p>	<p>David Baker <i>Sr. Manager, Professional Practices</i> Sara Lee</p> <p>Aaron Parks, CISA, CISM <i>Associate Director—Risk & Controls</i> Northwestern University</p> <p>Paul Phillips, CISA, CISM <i>Director, IS Customer Advocacy</i> General Growth Properties</p> <p>Ken Schmidt, CISA <i>Internal Audit Manager</i> The Options Clearing Corporation</p>	<p>If you plan to take the 2010 Certified Information Systems Auditor™ (CISA®) exam, then you will want to attend this workshop! Designed to assist and enhance the study process of CISA candidates, the CISA Review Weekend will address key IT audit issues and concepts. This two-day review will emphasize the technical job domain issues likely to receive extensive coverage on the CISA exam. Participants will receive the <i>CISA Review Manual 2010</i>, a comprehensive study manual with more than 350 questions, published by ISACA. This workshop will include a drill-down review of key technical issues likely to be addressed on the 2010 exam. Note: this workshop is a supplement to an intensive, multi-week chapter review program.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Know the study process to prepare for the 2010 CISA exam • Identify key issues covered on the exam • Discuss issues and concepts related to current IT audit practices • Understand automated IT audit, control and security practices • Identify IT audit concepts and issues addressed on the exam
WS2	<p>Remote Security Testing for Web Applications—Demonstration Based (two-day)</p> <p>I</p> <p>Saturday, 17 April and Sunday, 18 April</p>	<p>David Rhoades <i>Senior Consultant</i> Maven Security Consulting Inc.</p>	<p>If you are auditing Web application security, developing Web applications, or managing the development of Web applications, then this workshop is for you. Security testing helps to fulfill industry best practices and validate implementation, and is especially useful as it can be done at various phases within the application's lifecycle. In this two-day workshop you will learn how to test the security of web-based applications from the perspective of the end user. You will also learn how to use the tools and techniques needed to remotely validate a web application's security. The most popular threats and their potential impact will be covered, as well as the recommended prevention and mitigation steps you need to ensure security in your enterprise. Demonstrations and labs will be used to teach the tools and techniques needed to remotely detect and validate the presence of these threats.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Identify tools and techniques in security testing • Understand OWASP Top Ten & WASC Threat Classes • Identify and understand the vulnerability categories • Implement real-world testing advice and strategies

Did you know...

ISACA is pleased to announce a new risk-related certification. Certified in Risk and Information Systems Control™ (CRISC™). The CRISC designation is designed for IT professionals who identify and manage risks through the development, implementation and maintenance of information system control. The grandfathering program will open in April. For more information, please visit www.isaca.org/crisc.

Preconference Workshops

SESSION #	WORKSHOP TITLE	PRESENTER	DESCRIPTION:
WS3	<p>Risk IT Management (two-day)</p> <p>I</p> <p>Saturday, 17 April and Sunday, 18 April</p>	<p>Brian Barnier, CGEIT <i>Principal</i> ValueBridge Advisors</p> <p>Urs Fischer, CISA</p>	<p>Are you responsible for and/or does your role relate to IT governance and/or risk management in your enterprise? If so, you will benefit greatly from this workshop. Effective management of business risk has become an essential component of IT governance. Leading the drive to help enterprises mitigate risks, ISACA has developed a new IT enterprise risk management (ERM) framework, Risk IT. 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. It introduces ISACA's new Risk IT framework and the process model that includes risk governance, risk evaluation, and risk response. The workshop explains how ISACA's new framework relates to CoBIT and how it can help to achieve best practices in IT risk management. It examines the implementation and operational issues of ISACA's new Risk IT framework. The workshop explores how to integrate IT risk management into ERM, establish and maintain a common risk view, and make risk-aware business decisions. Finally, the workshop elaborates on 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.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Describe the principles of IT risk management • List the components of ISACA's new Risk IT framework • Apply the concepts of the model to realize its full business benefits and outcomes • Explain how the new Risk IT framework relates to CoBIT • Evaluate implementation and operational issues • Integrate IT risk management with ERM • Establish and maintain a common risk-view and make risk-aware business decisions • Maintain an operational risk profile, assess and respond to risk • Collect event data, monitor risk and report exposures and opportunities • Recognize how the Risk IT framework can help achieve best practices in IT risk management
WS4	<p>How to Audit and Secure Microsoft SQL Server (one-day)</p> <p>I</p> <p>Saturday, 17 April</p>	<p>John Tannahill, CISM, CGEIT <i>Management Consultant</i> J. Tannahill & Associates</p>	<p>Do you want to learn more about SQL? In this workshop, you will! The focus of this workshop will be on the audit, control and security issues related to the use of Microsoft SQL Server 2005. Learn practical approaches and techniques for evaluating the implementation of database security and control. Discussion includes SQL Server 2008 Security features. Live demonstrations using a Microsoft SQL Server environment will reinforce the principles presented.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Discuss architecture and components, audit and control objectives, and security configuration • Understand server and database roles, identification and authentication, and password administration • Recognize statement and object permissions • Discuss SQL Profiler, audit trails and security logs • Understand the role of operating system security • Identify known security vulnerabilities and security patches

Did you know...

Information Security Media Group (ISMG) conducted its first annual Information Security Today Career Trends survey. Based on the survey results, the list of top 10 certifications most sought after by security professionals in 2010 includes ISACA's CISA and CISM certifications.

Preconference Workshops

SESSION #	WORKSHOP TITLE	PRESENTER	DESCRIPTION:
WS5	Using CoBIT in IT Audit and Assurance (one-day) I Sunday, 18 April	Donald Caniglia, CISA, CISM, CGEIT <i>Senior Associate</i> Jon Campbell & Associates	Have you wanted to further your understanding of CoBIT, and how it relates to IT audit and assurance? Well, now you can! This one-day workshop will address how to use CoBIT for conducting IT assurance engagements, and will increase your understanding of the core concepts of control, IT assurance and IT governance. In addition, it will address the core concepts of an assessment of the effectiveness of controls. Participants will receive ISACA's IT Assurance Guide: Using CoBIT®, which will serve as the basis for discussion and guidance on how CoBIT can be used to support a variety of assurance activities, such as planning, scoping and assessing risks, and how to perform an assurance review of the CoBIT processes. The workshop will conclude with a discussion on how to document and communicate the business impact of control weaknesses. After completing this workshop, you will be able to: <ul style="list-style-type: none"> • Understand how to use CoBIT for conducting IT assurance engagements • Discuss the core concepts of control, IT assurance and IT governance • Comprehend how CoBIT can be used to support assurance activities • Perform an assurance review of the CoBIT processes • Document and communicate the business impact of control weaknesses

Postconference Workshops

(One-day) Please note: all postconference workshops will be held in two half-day sessions, Thursday afternoon and Friday morning.

SESSION #	WORKSHOP TITLE	PRESENTER	DESCRIPTION:
WS6	IT Controls Monitoring (one-day) I Thursday, 22 April and Friday, 23 April	Michael Garber, CGEIT Garber Associates Kenneth Vander Wal, CISA <i>Partner (retired)</i> Ernst & Young	In January 2009, COSO introduced Internal Control—Integrated Framework: Guidance on Monitoring Internal Control Systems. ISACA contributed to the three volume publication with IT-specific considerations, and is creating its own guidance that focuses on monitoring IT controls. This one-day workshop discusses the concepts and terminology of IT controls, automated controls and how to monitor them effectively. It explores how IT controls monitoring is an integral part of corporate risk management and of achieving business objectives. The workshop examines the IT controls monitoring tools, techniques and approaches and how to incorporate them into the internal audit process. It provides guidance on how monitoring affects large and small/medium enterprises and identifies how monitoring can benefit compliance efforts beyond Sarbanes-Oxley. The workshop introduces new research ISACA is conducting on the topic and shares the guidance developed from the project. After completing this workshop, you will be able to: <ul style="list-style-type: none"> • Evaluate the new guidance ISACA is developing in regards to IT controls monitoring • Identify key controls as candidates for an IT monitoring project • Differentiate between direct and indirect controls • Prepare an IT monitoring project plan • Use monitoring for verification of and sustaining IT controls • Use IT to monitor business controls • Use appropriate tools to increase the effectiveness of the IT controls monitoring effort • Incorporate IT controls monitoring tools and techniques into the internal audit process

Postconference Workshops

SESSION #	WORKSHOP TITLE	PRESENTER	DESCRIPTION:
WS7	Security and Audit of Oracle in Today's Enterprise (one-day) I Thursday, 22 April and Friday, 23 April	John Tannahill, CISM, CGEIT <i>Management Consultant</i> J. Tannahill & Associates	<p>This workshop will focus on the audit, control and security issues related to the use of Oracle database management systems in today's business environments. It will examine the security and audit issues of Oracle 10g / 11g environments. A particular focus of the workshop will be the differences in security mechanisms between the two versions. Participants will learn practical approaches and techniques for evaluating the implementation of database security and control. The workshop will use Oracle 10g and 11g database environments to demonstrate key security mechanisms and the use of Oracle audit scripts and tools. The workshop will cover the practical implementation and use of the Oracle audit trail mechanisms, the control issues with the Oracle system, and object privileges.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Discuss Oracle initialization parameters of security significance, as well as Oracle identification and authentication mechanisms • Use Oracle profiles to implement password control features • Identify key network security issues including Oracle listener security, known Oracle security vulnerabilities and how to test for their existence • Check for implementation of Oracle security patches • Recognize audit approaches to Oracle environments, including sample audit and security review checklists • Understand Oracle audit tools and techniques, as well as how to audit default Oracle user accounts and passwords
WS8	GRC: Managing the Corporate IT Portfolio (one-day) I Thursday, 22 April and Friday, 23 April	AI Marcella Jr., CISA <i>Business Automation Consultants LLC</i>	<p>The combination of business changes driven by market demands, enterprise responses (in terms of IT-intensive organizational changes), and technologies dispersed into business units, creates a need to explore how IT is most effectively and efficiently governed. IT governance may be defined as a framework for the ongoing leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that IT supports and enables the achievement of both IT and organizational strategies and objectives. This workshop addresses the critical correlation between proactive IT governance and practical IT portfolio management.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Map business and IT assets into a portfolio representation • Use portfolio representations as a communication tool among various parts of the business, the IT group, and the executive office • Recognize the inter-relationships between governance, risk and compliance as a means to effectively govern IT • Identify and categorize IT investments according to their levels of necessity and risk • Evaluate the line items in an IT portfolio. The line-items constitute the applications, or the infrastructure elements, or the IT services, or the development projects • Detect elements of continuing disconnects between the business leadership and their IT assets and resources • Assess whether these disconnects get in the way of successful exploitation of IT by businesses • Determine the responsiveness of IT to the needs of users and the enterprise • Pinpoint gaps between business management and IT management impeding effective communication and partnership • Ascertain whether business and IT are aligned culturally and that it is consistent with the strategic and competitive use of IT needed in the business
WS9	Harmonizing Standards—Achieving Compliance With Security Regulations (one-day) I Thursday, 22 April and Friday, 23 April	Todd Fitzgerald, CISA, CISM, CGEIT <i>Senior Technical Compliance Advisor</i> National Government Services	<p>Do you have questions about how to achieve balance among the different standards? If you do, then this is the workshop for you!</p> <p>This workshop provides an overview of each of the laws and regulations facing information security and provides approaches to achieving compliance by utilizing the control frameworks that are in place. This is a practical session that will explore different ways to meet the control standards of each standard. This workshop will dive into the controls and how to meet them for your enterprise.</p> <p>After completing this workshop, you will be able to:</p> <ul style="list-style-type: none"> • Articulate the various laws and regulations (HIPAA, SOX, PCI, GLBA, FISMA, ARRA, Red Flags Rule, etc.) impacting Security • Leverage CoBIT, ISO 27000, NIST 800-53, DISA standards/control frameworks to achieve compliance • Create security deliverables relevant to your own organization • Implement an 11-step security compliance model • Change the enterprise's approach to compliance from Board of Directors to end users

General Information

Venue and Accommodations

The North America CACS Conference will be held in Chicago, Illinois at the Hyatt Regency Chicago.

Hyatt Regency Chicago

151 E. Wacker Drive
Chicago, IL 60601
Telephone number: +1.312.565.1234
Fax: +1.312.239.4414
Web site: www.chicagoregency.hyatt.com
Guest room rate: US \$229 single/double
Guest room cut-off date: 14 March 2010

Why not stay in the heart of the conference action at a discounted hotel price? To guarantee you receive the discounted price, it is highly recommended that you make your reservations as soon as possible as our hotel block may sell out before the cut-off date. To make your reservations, please contact the hotel directly.

Conference and Workshop Pricing

Register by 10 February 2010 to receive the early-bird rate!

Conference

Member early-bird	US \$1550
Member	US \$1750
Nonmember early-bird	US \$1750
Nonmember	US \$1950

Workshops

One-day

Member	US \$550
Nonmember	US \$750

Two-day

Member	US \$750
Nonmember	US \$950

Register online now at www.isaca.org/nacacs.

Registration Dates and Hours

Preconference Workshop Registration

Saturday, 17 April 2010	7:30 a.m.–12:00 p.m.
Sunday, 18 April 2010	7:30 a.m.–12:00 p.m.

Conference Registration

Sunday, 18 April 2010	3:00 p.m.–7:30 p.m.
Monday, 19 April 2010	7:00 a.m.–5:00 p.m.
Tuesday, 20 April 2010	7:30 a.m.–5:00 p.m.
Wednesday, 21 April 2010	8:00 a.m.–5:00 p.m.
Thursday, 22 April 2010	8:00 a.m.–12:00 p.m.

Postconference Workshop Registration

Thursday, 22 April 2010	8:00 a.m.–5:00 p.m.
Friday, 23 April 2010	8:00 a.m.–12:30 p.m.

Conference Dates and Times

Preconference Workshops

Saturday, 17 April 2010	9:00 a.m.–5:00 p.m.
Sunday, 18 April 2010	9:00 a.m.–5:00 p.m.

Conference

Monday, 19 April 2010	8:30 a.m.–5:00 p.m.
Tuesday, 20 April 2010	8:30 a.m.–5:00 p.m.
Wednesday, 21 April 2010	8:30 a.m.–5:00 p.m.
Thursday, 22 April 2010	8:30 a.m.–12:00 p.m.

Postconference Workshops

Thursday, 22 April 2010	1:30 p.m.–5:00 p.m.
Friday, 23 April 2010	9:00 a.m.–12:30 p.m.

Program Benefits

Your North America CACS registration fee includes:

- Attendance at the conference sessions of your choice
- A complete set of electronic proceedings that includes session presentations received by the production deadline
- An opportunity to earn up to 44 continuing professional education (CPE) credit hours
- Complimentary continental breakfast for conference attendees Monday, 19 April through Thursday, 22 April
- Complimentary lunches Monday, 19 April through Wednesday, 21 April
- Complimentary morning and afternoon refreshment breaks
- Unlimited entry to the *InfoExchange* exhibits
- Invitations to all social and networking events:
 - Welcome Reception
 - Exhibitors' Reception
 - Special Evening Event

Social and Networking Events

Welcome Reception

Sunday, 18 April 2010 5:30 p.m.–7:30 p.m.
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.

Exhibitors' Reception

Tuesday, 20 April 2010 5:00 p.m.–7:30 p.m.
The Exhibitors' 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.

Special Evening Event

Wednesday, 21 April 2010 6:30 p.m.–10:30 p.m.
Join us for a special evening at the world famous John G. Shedd Aquarium for food, cocktails and an outstanding assortment of live aquatics. The conference delegation will spend the evening among the various aquatic exhibits of the Shedd Aquarium. The evening will begin in the Oceanarium and end in the historical Caribbean Reef Rotunda. This will be a memorable location for the conferences main networking event. Admission to the event, food and beverage and transportation is included with your conference registration. Guest tickets are available for purchase for \$125 per ticket.

General Information

Exhibitor Educational Sessions

Tuesday, 20 April 2010 5:30 p.m.–7:30 p.m.
Wednesday, 21 April 2010 10:15 a.m.–12:15 p.m.
Interact with the exhibitors and earn CPE hours. ISACA offers special one-half-hour sessions presented by the *InfoExchange* exhibitors. Exhibitor 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.

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 **24 March 2010** 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, in addition to any applicable membership dues that would be applied if you checked the box marked: "I wish to apply the difference between member and nonmember fees toward a membership in ISACA". No refunds can be given after **24 March 2010**. 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
E-mail: conference@isaca.org

Go Green

In an effort to conserve paper, ISACA conferences have gone green! Upon registration, ISACA conference attendees will receive a flash drive containing the most current conference presentation materials available. This will allow attendees to view presentations on their laptops and make notes during the conference. Attendees will receive online access to all available conference presentations two weeks prior to the conference, enabling them to view the presentations they are interested in or print hard copies to bring to the conference. Please note: printing stations will not be provided onsite at the conference. If you have any questions, please contact the conference department at conference@isaca.org or +1.847.660.5585.

Not a member of ISACA? Join today!

When you register for the conference as a nonmember, the difference between member and nonmember conference fees can be applied towards ISACA membership. This means you can become a member at the international and chapter level for little to no additional cost; it just depends on your local chapter dues. To take advantage of this great offer, check the box on the registration form. For more information about ISACA membership, visit the web site at www.isaca.org/membership or contact the membership department at membership@isaca.org.

NOTE: This offer expires 30 days after completion of the event. Nonmembers pay the nonmember conference fee when registering.

Registration Methods

Choose one of four easy ways to register:

1. **ONLINE** at www.isaca.org/nacacs
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, IL 60603
ABA #0260-0959-3
ISACA Account #22-71578
S.W.I.F.T. code BOFAUS3N
[Please include **attendee's name** and **NACACS** on the Advice of Transfer.]

Dress

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

Continuing Professional Education Credits

To maintain Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®) and Certified in the Governance of Enterprise IT® (CGEIT®) certifications, certification holders are required to earn 120 CPE credit hours over a three-year period in accordance with ISACA's continuing professional education (CPE) policy. Attendees can earn up to 44 CPE credits; 23 by attending the North America CACS Conference and an additional 7 CPE credits for attending each day of optional pre- or postconference 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, 150 Fourth Avenue North, Suite 700, Nashville, TN, 37219-2417 or by visiting the web site: www.nasba.org.

Disclaimer

The information in this brochure is correct at the time of printing. ISACA reserves the right to alter or delete items from the program in the event of unforeseen circumstances. Material has been prepared for the professional development of ISACA members and others in the IT audit, control, security and governance community. Neither the presenters nor ISACA can warrant that the use of material presented will be adequate to discharge the legal or professional liability of the members in the conduct of their practices. All materials used in the preparation and delivery of presentations on behalf of ISACA are original materials created by the speakers, or otherwise are materials which the speakers have all rights and authority to use and/or reproduce in connection with such presentation and to grant the rights to ISACA as set forth in speaker agreement. Subject to the rights granted in the speaker agreement, all applicable copyrights, trade secrets, and other intellectual property rights in the materials are and remain with the speakers.

Please note: unauthorized recording, in any form, of presentations and workshops is prohibited.

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.



2010 North America Conference

18-22 April 2010 • Chicago, Illinois, USA

Registration Form

Page 1 of 2

NAC2010

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) _____ E-mail Address _____

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

Address _____

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

Please do NOT include my full address on the roster given to delegates, speakers and exhibitors.

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 nonmember 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.)

CONFERENCE TRACKS	Preconference Workshops														Postconference Workshops	
	Sat. 17 April	Sun. 18 April	Mon. 19 April			Tue. 20 April				Wed. 21 April			Thu. 22 April		Fri. 23 April	
	9:00 a.m.–5:00 p.m.	9:00 a.m.–5:00 p.m.	10:30 a.m.–12 Noon	1:30 p.m.–3:00 p.m.	3:30 p.m.–5:00 p.m.	8:30 a.m.–10:00 a.m.	10:30 a.m.–12 Noon	1:30 p.m.–3:00 p.m.	3:30 p.m.–5:00 p.m.	8:30 a.m.–10:00 a.m.	1:30 p.m.–3:00 p.m.	3:30 p.m.–5:00 p.m.	8:30 a.m.–10:00 a.m.	10:30 a.m.–12 Noon	1:30 p.m.–5:00 p.m.	9:00 a.m.–12:30 p.m.
Track 1 IT Audit Core Competencies	WS1	111	121	131	211	221	231	241	311	321	331	411	421	WS6		
Track 2 IT Audit Tools and Competencies		112	122	132	212	232	312	322	332	412	422					
Track 3 Techniques for Evaluating Business Practices and Professional Development	WS2	113	123	133	213	223	233	243	313	323	333	413	423	WS7		
Track 4 Emerging Issues and ISACA Research		114	124	214	224	234	244	314	324	334	414	424				
Track 5 IT Governance and Compliance	WS3	115	125	215	225	235	245	315	325	415	425	WS8				
Track 6 Information Technology Security and Data Protection		116	126	216	226	236	246	316	326	416	426					
Track 7 IT Risk and Exposure Management	WS4	WS5	117	127	217	227	237	317	327	417	427	WS9				



2010 North America Conference

18-22 April 2010 • Chicago, Illinois, USA

Registration Form

Page 2 of 2

NAC2010

Attendee Name _____

2. Registration Fees (All fees are quoted in US dollars.)

Please circle your choices below

Conference

Register by 10 February 2010 to receive the early-bird rate!

Member early-bird	\$1,550
Member	\$1,750
Nonmember early-bird	\$1,750
Nonmember	\$1,950

Pre- and Postconference Workshops

Two-day Workshop

- WS1—CISA Review Weekend
- WS2—Remote Security Testing for Web Applications—Demonstration Based
- WS3—Risk IT Management

Member	\$750
Nonmember	\$950

One-day Workshop

- WS4—How to Audit and Secure Microsoft SQL Server
- WS5—Using COBIT in IT Audit and Assurance
- WS6—IT Controls Monitoring
- WS7—Security and Audit of Oracle in Today's Enterprise
- WS8—GRC: Managing the Corporate IT Portfolio
- WS9—Harmonizing Standards—Achieving Compliance with Security Regulations

Member	\$550
Nonmember	\$750

Guest Ticket for Special Evening Event (Wed., 21 April) _____ @ US \$125.00 = US \$ _____

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

3. Indicate Method of Payment

Payment enclosed. Make cheque payable in US dollars, drawn on a US bank, payable to ISACA.

Wire Transfer in US dollars Date Transferred _____
(NOTE: Wire transfers and mailed cheques 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.)

Number _____ Expiration Date _____

Name of Cardholder _____

Signature of Cardholder _____

Complete Billing Address of Cardholder (if different from above)

4. Registration Methods

- A.  REGISTER ONLINE at www.isaca.org/nacacs.
- 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, SWIFT code BOFAUS3N

[Please include **Attendee's Name** and **NACACS** on the Advice of Transfer.]

5. Cancellation Policy

All cancellations must be received by **24 March 2010** either by phone, fax or e-mail in order to receive a refund of conference registration fees less a US \$100 cancellation charge and workshop registration fees less a US \$50 cancellation charge and, if applicable, less the amount applied to membership dues as a result of checking the box marked: "I wish to apply the difference between member and nonmember conference fees toward a membership in ISACA." No refunds will be given after **24 March 2010**. Attendee substitution is permitted at any time until the conference. Substitution of a nonmember for a member will result in 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, such as complaints and/or refunds, please contact the ISACA conference department by phone at +1.847.660.5585, fax at +1.847.253.1443, or e-mail at conference@isaca.org.

6. Special Arrangements

Special Dietary Requirements _____

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

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.

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Please share this brochure with

- CISAs, CISM's, CGEIT's
- IT auditor
- Information security professional
- IT governance professional
- Compliance professional
- IT risk professional
- External auditor/accountant
- Audit director/manager
- IT security director/manager
- Chief audit executive/general auditor



**North America Computer Audit,
Control and Security Conference**

18–22 April 2010
Hyatt Regency Chicago
Chicago, Illinois, USA



www.isaca.org/nacacs

2010 North America CACS Conference Task Force

- Jeffrey M. Krull, CISA** (Chair)
Senior Manager, PricewaterhouseCoopers
- Brian Barnier, CGEIT**
Consultant, ValueBridge Advisors
- Michael A. Berardi, Jr., CISA, CGEIT**
Senior Audit Manager, Nestlé
- Michael E. Juergens, CISA, CGEIT**
Principal, Deloitte & Touche
- Harshul Joshi, CISA, CISM, CGEIT**
Director, Information Technology, CBIZ Inc.
- Steve Orrin**
Director Security Solutions, Intel
- Lorraine Peoples, CISA**
Vice President—Internal Control Department, Estee Lauder Companies Inc.
- John Galloway Tannahill, CISM, CGEIT**
Management Consultant, J. Tannahill & Associates

**2010 North America CACS Partnering Chapter
Task Force Members**

- Ken Schmidt, CISA** (Chair)
The Options Clearing Corp.
- Robert Pardon**
Resources Global Professionals
- Jan Hertzberg, CISA**
Grant Thornton
- Jill Frisby, CISA**
Crowe Horwath LLP
- Erika Del Giudice, CISA**
Crowe Horwath LLP
- Norman Spielman, CISA**
The Warranty Group