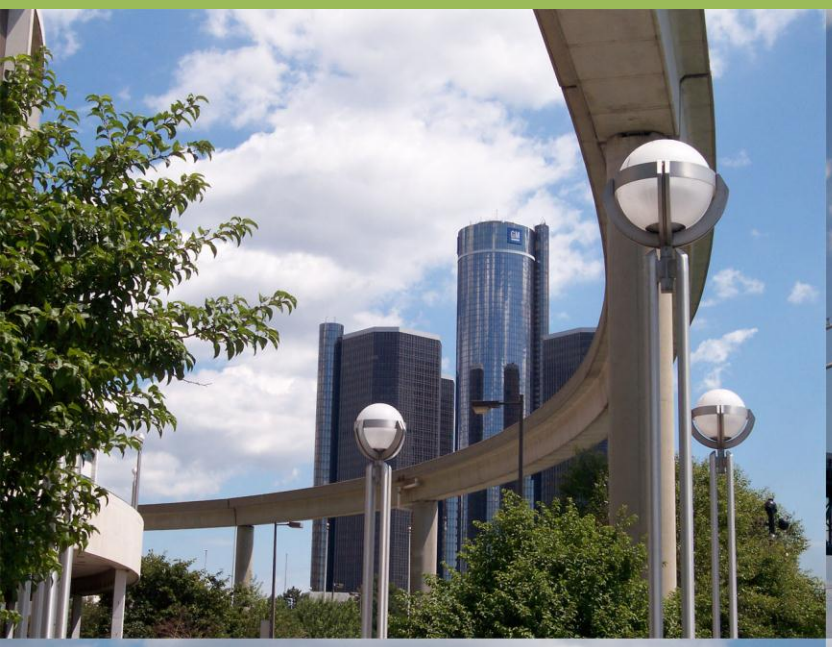
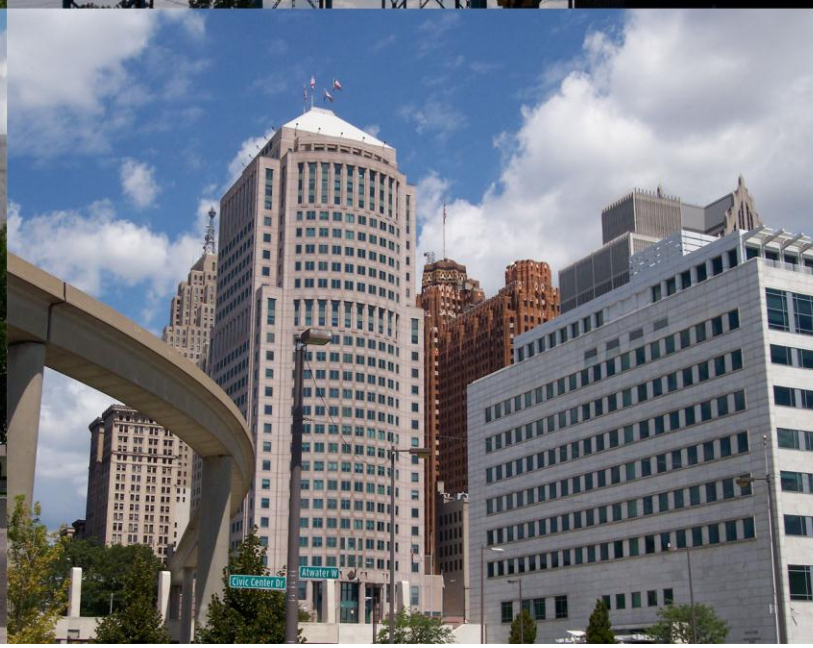
14TH ANNUAL

IIA and ISACA Spring Conference





MARCH 11-13, 2013

University of Michigan-Dearborn

Fairlane Center

The Institute of Internal Auditors Detroit Chapter

ISACA® Trust in, and value from, information systems Detroit Chapter

Welcome

If you are responsible for your company's internal auditing, information systems security and integrity, accounting, finance, Sarbanes-Oxley compliance or other regulatory matters, or simply getting back to the basics, you will want to join us for the 14th annual Detroit Spring Conference.

The Detroit Chapters of the IIA and ISACA are proud to co-sponsor the annual Spring Conference. Each year, the conference committee spends a considerable amount of time planning a comprehensive series of course offerings for our members and guest. The 2013 event is no exception.

A number of classes sell out each year. Don't miss this opportunity to network with your peers, enhance your skills, and learn about new products and services in the marketplace! Our goal is to provide a training conference of world-class caliber tailored to your needs.

We look forward to seeing you at the Spring Conference.

- *The 2013 Spring Conference Committee*

RETURNING THIS YEAR! – VENDOR EXPO

We have invited many audit and assurance vendors to set up displays during the conference giving you an opportunity to learn about products and partners that are in the marketplace and their associated benefits for your organization.

A Special Thanks to our Platinum Sponsors who continue to give generous support to this annual event!

Monday Lunch– PwC
Tuesday Lunch – Experis Finance
Wednesday Lunch – TBD
Breakfast Each Day – TBD

CONFERENCE PROGRAM

TRACK	MON MARCH 11	TUES MARCH 12	WED MARCH 13
A	Outstanding Presentation and Meeting Facilitation Skills (Dr. Joan Pastor)		Communication and Personal Management Skills (Dr. Joan Pastor)
B	Forensic Analytics, Techniques and Investigation (Mark Nigrini, PhD)		
C	Successful Fraud Investigations – Avoiding Pitfalls, Navigating Risks, and Achieving Results (Paul Zikmund)		Conducting Effective Fraud Risk Assessments (Paul Zikmund)
D	Auditing the Business Case and Governance of Social Media (Norm Kelson)	IT Auditing Principles for Internal Audit (John Beveridge)	
E	Risk Based Internal Auditing (Greg Duckert)		
F	Bank Internal Audit University (Dennis Cox)		
G	Advanced Auditing for In-Charge Auditors (Joel Kramer)		
H		Big Data: How to Control (Not Fight) It (Jeff Kalwerisky)	Threat Modeling: Finding Security Threats Before They Happen (Jeff Kalwerisky)
I	Network Security Fundamentals (John Tannahill)	Audit & Security of Wireless and Mobile Technology (John Tannahill)	
J	Assessing your Protection of PII (Jeff Kalwerisky)	Auditing IT Application Systems (Norm Kelson)	
K	Taking the Bulls-Eye Off Your Website: How to Audit Modern Web Applications (Ken Cutler)		
L	Advanced SAP (Steve Biskie)		

TRACK A -1
OUTSTANDING PRESENTATION AND MEETING FACILITATION SKILLS
(DR. JOAN PASTOR, MONDAY - TUESDAY)
15 CPEs

Seminar Focus and Features

Research indicates that presentation skills are critical to not only jobs where presentations are given, but also overall career success. If you conduct meetings or formal presentations, you need this course. Auditors can benefit from this course immensely by learning skills needed to be effective during opening, interim and closing conferences, as well as the numerous special projects requiring formal presentations.

In this two day seminar, the focus is on understanding the different types of presentations one can give (depending on the results you want to achieve), how to get the type of presentation you want down on paper in an appropriate format, and then practicing in front of others. Attendees will receive coaching, work on presentations, and then present portions of their presentations. Constructive feedback and additional coaching is provided after the delivery of the presentations.

Some of the areas covered include:

- Difference between presenting and facilitation, and where each fits into auditing
- Body and verbal language
- Handling difficult situations
- Connecting with your listeners and clients
- Persuasive vs. informational talks, and how to gain buy-in through presentation skills

People will leave with a clear understanding on how to conduct an excellent presentation, a better understanding of their personal strengths and challenge areas, and an increased confidence level for handling different types of presentations and group situations.

Prerequisite: Attendees usually bring in material to use in a presentation

Learning Level: Basic

TRACK A -2
COMMUNICATION AND PERSONAL MANAGEMENT SKILLS
(DR. JOAN PASTOR, WEDNESDAY)
7 CPEs

Seminar Focus and Features

Auditing is not easy. There can be many demands put on an auditor; likewise, the auditor can put a lot of demands on others. This special one-day course addresses some challenging situations (and people) that auditors often face, and focuses on developing the specific skills needed to build and maintain confidence while reducing stress!

In this course you will learn:

- The secret ingredients for building confidence and maintaining it
- How to manage anxiety and stressful situations / reactions
- The four components for successfully handling emotions
- A step-by-step process for changing behavior in yourself and others
- Five specific and concrete tools used in: building confidence, gaining a sense of competency, and keeping calm and positive in various situations (for example, when giving bad news, when others react negatively or disagree, when making requests of people for their time and resources)
- How to communicate in ways that enhance people's willingness to listen to you
- Practice special, subtle techniques for maintaining a positive outlook and communicating effectively in challenging situations

Learning Level: Basic

About the Instructor

Joan Pastor, PhD

Joan Pastor, Ph.D., is president of JPA International, Inc., and has been a professional international speaker, trainer and coach since 1979. She is well-known for her training, facilitation, and consulting skills, and has worked with numerous organizations to develop their vision and then apply the strategies and processes to achieve it. Joan is a certified speaking professional (CSP) and also a certified mediator, and has mediated numerous workplace and business conflicts over the years. Her book, "Conflict Management and Negotiation Skills for Internal Auditors" was published in 2007 by The Institute of Internal Auditors. Her article "The Eight Habits of Highly Effective Audit Committees" received the AICPA Excellence in Journalism Award in 2008.

The recipient of numerous awards, Joan has been working with the IIA chapters, congresses and conferences since 1987 and with the AICPA and ACFE since 1998.

Joan and her associates focus on developing all the people, communication, organizational and leadership skills associated with these professions. She has also made pioneering contributions related to fraud and the white collar criminal, ethics, fraud risk-assessment and business process management and its application to organizational change (downsizing, fast growth, mergers & acquisitions). Her consulting projects in collaboration with audit departments have ranged from redesigning the major business processes for a major airline, redesigning a faulty 360-degree performance management process, facilitating the acquisition and merger of several hospitals and a college with another major university, and assisting in re-engineering risk assessment programs.

When the Enron debacle blew open, Joan unleashed the model that she had been working on for over 10 years on the psychology behind fraud and unethical people in business. It has been extremely well received from CFEs to Audit Committees to the FBI to senior executive teams. Joan often works alongside legal counsel, audit and executives on potential or discovered fraud situations, and has uncovered three embezzlement and fraudulent schemes on her own as well.

TRACK B
FORENSIC ANALYTICS, TECHNIQUES AND INVESTIGATION
(MARK NIGRINI – MONDAY - TUESDAY)
15 CPEs

Seminar Focus and Features

This workshop draws on the topics covered in *Forensic Analytics* by Mark Nigrini. Forensic analytics is the procurement and analysis of electronic data to reconstruct, detect, or otherwise support a claim of financial fraud. Other goals include the detection of errors, inefficiencies, and biases where people tend towards certain behaviors (perhaps favoring specific numbers or number ranges) to influence decision makers or to circumvent actual or perceived internal control thresholds.

This is a special opportunity to learn about Benford's Law and other forensic analytic tools and techniques. No prior forensic or analytics experience is assumed. The first-day topics include Benford's Law, a corporate payments case study, continuous monitoring using risk-scoring, three fraud and tax evasion case studies, and a finale on software solutions that will raise your forensic efficiency and effectiveness. Most of the second day is devoted to hands-on time with actual relevant case studies. These sessions use real-world, value-added hands-on case studies with discussion and multiple choice questions to reinforce the forensic material with an energetic conclusion that is a summary of the main points and a look at aspects of the legal environment that play a role in the prosecution of fraud cases. Here Nigrini makes a compelling case for effective internal controls and an efficient, capable, and competent proactive fraud detection regime.

Bring your laptops on the second day to work along with the instructor for the case studies.

Learning Level: Basic

About the Instructor

Mark Nigrini, Senior Fellow

Mark J. Nigrini, PhD, is a professor at The College of New Jersey where he teaches managerial accounting, auditing, and forensic accounting. Benford's Law has been his research passion since his days as a Ph.D. student at The University of Cincinnati.

Nigrini's current research addresses advanced theoretical work on Benford's Law, applications of forensic analytics to contemporary topics such as the detection of Ponzi schemes, financial statement fraud, LIBOR manipulations, and the legal framework of fraud convictions.

Nigrini is the author of Forensic Analytics (Wiley, 2011) which describes analytic tests to detect fraud, errors, estimates, and biases in financial data. He is also the author of Benford's Law (Wiley, 2012) which is the seminal work on applications of Benford's Law. His next book "*Losing the War against Fraud*" will be published in 2013.

His work has been featured in national media including The Financial Times, New York Times, and The Wall Street Journal and he has published papers on Benford's Law in accounting academic journals, scientific journals, and pure mathematics journals, as well as professional publications such as Internal Auditor and Journal of Accountancy.

His radio interviews have included the BBC in London and NPR in the United States. His television interviews have included an appearance on NBC's Extra. He was interviewed in July for a television program on fraud for the Investigation Discovery Channel. He regularly presents professional seminars for accountants and auditors in the U.S. and Canada, Europe, and Asia with recent events in Singapore, Malaysia, and New Zealand.

TRACK C - 1
SUCCESSFUL FRAUD INVESTIGATIONS – AVOIDING THE PITFALLS, NAVIGATING RISKS, AND ACHIEVING RESULTS
(PAUL ZIKMUND – MONDAY - TUESDAY)
15 CPEs

Seminar Focus and Features

This two-day session is designed to provide participants with an understanding of the key elements of successful fraud investigations.

Participants will learn:

- What to do when you suspect fraud
- Key steps in investigating fraud should it occur at your organization
- Risks and pitfalls of fraud investigations
- How to navigate risks and avoid pitfalls

The course will also discuss various case studies, fraud scenarios and successful investigation techniques.

Learning Level: Basic

TRACK C - 2
CONDUCTING EFFECTIVE FRAUD RISK ASSESSMENTS
(PAUL ZIKMUND – WEDNESDAY)
7 CPEs

Seminar Focus and Features

Internal auditing is in an excellent position to identify fraud schemes and scenarios and evaluate the controls in place to prevent them. Regulations and guidance issued over the past several years have increased the need to implement controls designed to reduce the likelihood of fraud within an organization. To meet these requirements and reduce the risk of fraud, organizations should consider performing regular enterprise-wide fraud risk assessments.

Internal auditing is responsible for evaluating whether internal controls are designed to meet their overall objectives. This evaluation includes controls designed to reduce the risk of fraud. During this one-day session, participants will learn:

- How fraud risk assessments differ somewhat from the more conventional methods used to assess risk in that they are schemes- and scenarios-based, which requires experienced personnel who are familiar with the more common fraud schemes impacting today's organizations.
- An approach to conduct effective fraud risk assessments that includes evaluating the organization's fraud risks, identifying possible fraud schemes and scenarios, prioritizing identified fraud risks, and evaluating mitigating controls.

Learning Level: Basic

About the Instructor

Paul E. Zikmund, CFE, CFFA, CFD

Paul E. Zikmund serves as Director, Global Integrity & Forensic Audit, at Bunge in White Plains, NY. He is responsible for managing and conducting investigations of fraud and misconduct, implementing fraud detective techniques, administering the company's fraud risk assessment process, and managing anti-fraud programs and controls designed to reduce the risk of fraud within the company.

Prior to joining Bunge, Paul worked as the Senior Director Forensic Audit responsible for developing, implementing, and administering fraud risk management services at Tyco and to clients in Princeton, NJ, and as the Director Litigation Support Services at Amper, Politziner, & Mattia, LLP, in Philadelphia, PA.

He possesses nearly 20 years of experience in this field and has effectively managed global fraud and forensic teams at various Fortune 500 companies.

Paul, who is a Certified Fraud Examiner, Certified Fraud Deterrence Specialist, and Certified Forensic Financial Analyst, has designed and implemented programs to detect and investigate instances of fraud. Paul also conducts fraud risk assessments and fraud awareness training to help detect and deter fraud within their organizations. His public and private sector experience includes the investigation of complex financial frauds, conducting forensic audit engagements, and providing litigation support for a variety of industries.

Before joining Amper, Paul was a Principal, Fraud and Forensic Services at SolomonEdwardsGroup, LLC and a Senior Manager – Enterprise Risk Services with Deloitte and Touche, LLP. Prior to that, he served in a variety of in-house fraud and forensic investigative roles with The Dow Chemical Company, Nortel Networks, and Union Carbide Corporation. He began his career as a Municipal Police Officer, and then a State Trooper and Special Agent with the Attorney General's Office for the Commonwealth of Pennsylvania.

Paul received a Bachelor of Science degree in the Administration of Justice and a Certificate of Accountancy from The University of Pittsburgh. He continued his education with a Masters of Business Administration at the University of Connecticut and a Masters of Accountancy at Auburn University. Paul has authored various articles relating to fraud detection, prevention, and investigation. He speaks regularly at seminars and conferences on the topic of fraud and also teaches a graduate level fraud and forensic accounting course at Rider University in New Jersey and LaSalle University in Philadelphia.

TRACK D-1
AUDITING THE BUSINESS CASE AND GOVERNANCE OF SOCIAL MEDIA
(NORM KELSON – MONDAY)
7 CPEs

Seminar Focus and Features

Social media is one of the hottest topics in business today. We all hear about Facebook, Twitter, LinkedIn and other social media sites. How does a business translate these technologies/resources to a financially viable communication channel, and how does management evaluate its effectiveness? As auditors, evaluating social media results is certainly within scope. In this seminar we will answer these questions and prepare the auditor to perform an audit of social media from a governance, controls, and management perspective.

In this seminar, we will discuss:
- The definition of social media
- Who should be involved the planning and implementation of social media
- Metrics to evaluate the effectiveness of social media
- Guidelines for effectively managing social media
- Planning the audit of social media

Learning Objectives
- Understand what constitutes social media
- Aligning social media with business objectives
- How to evaluate the effectiveness of social media
- Establishing and implementing your audit objectives

Learning Level: Basic

About the Instructor

Norm Kelson, CPA, CISA, CGEIT

Norm Kelson, founder and President of CPE Interactive, specializes in building and disseminating best practices to assurance, risk, governance, and management stakeholders. With over 30 years of extensive experience in IT assurance and governance, he has served in a variety of capacities as a consultant with a Big 4 firm and an internal audit boutique, internal auditor executive, and industry advocate.

He is currently creating IT Audit/Assurance Programs for ISACA which are available as a resource to its members. He recently completed a series of case studies to support ISACA's IT Governance Using COBIT® and VAL ITTM: Student Book 2nd Edition, and is involved in other IT governance related projects for ISACA and the IT Governance Institute.

Norm was Managing Director of IT Audit and Technical Seminars for MIS Training Institute. During his 12 year tenure he was responsible for creation and curriculum development of its global IT Audit training portfolio focusing on best practices in risk-based auditing.

He has held positions as: Director of IT Audit at Ahold USA (Stop & Shop, Giant, Tops, and Peapod) and was a key member of the internal audit professional practices and standards and the global information security committees; Vice President of Internal Audit Services and National IT Audit Practice Director for CBIZ Harborview Partners; managed KPMG's New England Region IT Auditing practice, and held positions in IT Audit management with Fannie Mae, CIGNA, and Loews Corporation. He began his career as a financial auditor with Laventhol and Horwath.

Norm serves as an Adjunct Professor at Bentley University and is a member of the Audit/AIS Curriculum Committee.

He is a frequent speaker and subject matter expert at ISACA/ITGI and Institute of Internal Auditors (IIA) conferences, is a former Executive Vice President of the New England ISACA Chapter and currently serves on the Chapter's Strategic Planning Committee.

Norm received a Bachelor of Science in Business Administration from Boston University and an MBA from the University of Pennsylvania Wharton School. He is a Certified Public Accountant, Certified Information Systems Auditor, and Certified in the Governance of Enterprise Information Technology.

TRACK D-2
IT AUDITING PRINCIPLES FOR INTERNAL AUDIT
(JOHN BEVERIDGE – TUESDAY-WEDNESDAY)
15 CPEs

Seminar Focus and Features

Information technology is an integral part of all financial and business processes. The internal audit manager requires a fundamental understanding of IT's impact on the audit processes and associated risk to effectively drive the audit process. This training session is aligned with our staff-level courses, and utilizes the same basic outline, but has been designed for the internal audit manager.

Our focus will be:

- A managerial level understanding of IT concepts focusing on audit risk of IT controls on the audit process
- Integrating IT risks into the overall risk assessment
- Reliance on IT control activities
- Scoping and managing the application audit
- Staffing and skill set integration

As each topic is introduced and discussed, we will keep the level of detail appropriate to the internal audit manager and focus on the execution of the audit.

Learning Objectives

- Understand the IT risks and be able to apply these risks to audit planning
- Have the tools to manage integrated audit teams and align IT and financial audit findings
- Be able to consider and build IT audit findings into audit reports, framing the issue in terms relevant to senior management
- Understand how to evaluate opportunities to use computer audit assist techniques as a testing approach

Learning Level: Intermediate

About the Instructor

John W. Beveridge, CGFM, CISA, CISM, CFE, CGEIT, CRISC

John Beveridge is Director of IT Audit Training for CPE Interactive, and his professional career spans over twenty-five years in government and private industry in the United States and England, including over twenty years in IT audit management.

John is the former Deputy Auditor for the Commonwealth of Massachusetts, where he was responsible for the Information Technology Audit Division for the Massachusetts Office of the State Auditor and served as Co-Chair of the Commonwealth's Enterprise Security Board and member of the IT Advisory Board. He had served as a member of the Massachusetts Government Technology's Advisory Board, 2003 through 2009, Governor's Commission on Computer Crime, Governor's Commission on Computer Technology and Law, Governor's Task Force on E-Commerce, and the Governor's IT Commission.

He is a member of the adjunct faculty of Bentley University and Northeastern University, where he has taught courses in accounting information systems and IT auditing.

John has served as ISACA's International President, Vice President for Standards, member of various boards and committees including the COBIT® Steering Committee, Information Systems Auditing Standards Board, Education Board, Assurance Board, IT Governance Credentialing Committee, and the Advisory Committee to the Task Force on Model Curriculum for IT Auditing. John was instrumental in the development of COBIT's Control Objectives and Management Guidelines, co-authored a Control Practices Guideline for Information Systems Continuity Planning, and has authored professional standards for information systems auditing and work-related publications. He is a frequent lecturer on the implementation of COBIT®, IT auditing, planning and performing application system audits, and audit management.

He received a Bachelors of Science in economics from the University of Massachusetts and a Masters in Public Administration (MPA) with a major in Finance from Suffolk University. John is a Certified Governmental Financial Manager, Certified Information Systems Auditor, Certified Information Security Manager, Certified Fraud Examiner, Certified in Risk and Information Control Assurance specialist, and Certified in the Governance of Enterprise IT.

TRACK E
RISK-BASED INTERNAL AUDITING
(GREG DUCKERT – MONDAY - WEDNESDAY)
22 CPEs

Seminar Focus and Features

With the increasing emphasis on corporate governance initiatives and the release of recent ERM guides and pronouncements, there has never been a more critical time for auditors to expand their knowledge of risk management and assessment.

In this intensive three-day seminar you will learn the underlying concepts of a risk-based audit methodology. You will cover all aspects of risk assessment, including the fundamentals of risk-based auditing, defining risk in business terms, identifying key risk areas, evaluating global risk, and conducting a detailed risk analysis at the engagement level. You will explore a strategy for transitioning the department to a risk-based function as well as for re-educating management and the audit committee. Throughout the seminar you will work through risk drills that will allow you to put into practice what you have learned. You will leave this high-impact seminar with audit efficiencies and business insights that will maximize Audit's contributions to the organization, and cast IA as a value-adding member of the team.

Prerequisites: Fundamentals of Internal Auditing or equivalent experience

Learning Level: Intermediate

About the Instructor

Greg Duckert, CIA, CISA, CMA, CPA

Greg Duckert is CEO of Audit, Inc., a consulting firm specializing in risk assessment models, operational analysis, and audit process methodologies designed to maximize returns to the organization. Mr. Duckert is also a Senior Consultant for MIS Training Institute and has over 30 years of national and international experience as an Internal/IS Audit Director. Mr. Duckert has held Audit Director Positions in the manufacturing, construction and healthcare industries, assuming responsibilities for financial, operational, and information systems auditing functions. His information systems expertise includes application audits, software acquisition, systems development, controls, security design, adequacy and implementation, and systems operational efficiencies. He has performed consulting services in IS, financial, and operational audits, as well as in business acquisitions and start-ups.

TRACK F
BANK INTERNAL AUDIT UNIVERSITY
(DENNIS COX – MONDAY - WEDNESDAY)
22 CPEs

Seminar Focus and Features

This three-day seminar is designed to provide internal auditors with the critical skills they need to carry out successful assignments within financial service institutions. You will examine the various components of the banking industry and explore audit approaches appropriate for designing suitable audit programs for such assignments. You will gain a general understanding of the banking industry and applicable approaches to retail, corporate, and private banking; trade finance; and financial instruments. You will cover such timely topics as personal and corporate lending, security and provisioning, futures and the futures market, investment banking, and more. Throughout the seminar case studies will enhance what you learn.

Prerequisites: Some knowledge of basic audit techniques and of the financial markets is recommended.

Learning Level: Basic

About the Instructor

Dennis Cox, BSC, FCA, FISI

Dennis Cox, BSC, FCA, FISI, is the Founder and Chief Executive of Risk Reward Ltd., where he oversees all consulting and training projects and specializes in Basel Accord challenges surrounding credit, market, and operational risk. Previously, he was with HSBC Bank where he held senior management roles. Prior to joining HSBC Bank, he was Global Risk Manager at Prudential Portfolio Managers Ltd. Mr. Cox is the author of Banking and Finance: Accounts, Audit and Practice and co-author of The Mathematics of Banking & Finance.

TRACK G
ADVANCED AUDITING FOR IN-CHARGE AUDITORS
(JOEL KRAMER – MONDAY - WEDNESDAY)
22 CPEs

Seminar Focus and Features

In this three-day session you will learn all of the elements involved in traditional and operational risk-based auditing. With your peers, you will review such concepts as audit program flexibility, organizational and financial compliance risk assessment, priority setting during fieldwork, and effective oral and written communication of audit findings. You will cover preliminary fieldwork, audit program development, risk assessment, and auditing the control environment in today's business climate.

Prerequisites: Fundamentals of Internal Audit or equivalent experience

Learning Level: Intermediate

About the Instructor

Joel Kramer, CPA

Joel F. Kramer, CPA, is Managing Director of the Internal Audit Division of MIS Training Institute, responsible for developing MIS' internal audit curriculum. Formerly worldwide Director of Internal Audit at Instrumentation Laboratory, Mr. Kramer and his staff conducted operational and financial audits in the United States, Canada, Mexico, and throughout Europe. Prior to Instrumentation Laboratory, he had been Internal Audit Manager for the Gillette Company. Previously, Mr. Kramer spent five years with Coopers & Lybrand. A recognized speaker on internal audit topics, he has addressed many IIA Chapters. He is a member of the Board of Governors of the Greater Boston Chapter of the IIA. Mr. Kramer has written articles on productivity and project management for Internal Auditing Magazine and has developed two highly successful videos, Day One in Internal Auditing and Modern Audit Tools and Techniques.

TRACK H-1
BIG DATA: HOW TO CONTROL (NOT FIGHT) IT
(JEFF KALWERISKY - TUESDAY)
7 CPEs

Seminar Focus and Features

The term Big Data refers to very large collections of data sets, which typically contain structured data from database tables as well as more complex unstructured data often from multiple sources, such as documents and spreadsheets, emails, and text messages, "Tweets" and other social media, blogs, photographs, and virtually any source of electronic data.

As with most new technologies, Big Data presents new control and security problems. The situation is exacerbated by the other two current trends: (1) mobile devices are being used to gather and access Big Data from anywhere; and (2) use of public and private Clouds to host and analyze the Big Data sets. As the volume of data produced continues to accelerate, it is important for auditors and security practitioners to understand the special data security and privacy risks associated with Big Data environments, early in the process, and be able take appropriate steps to control and protect sensitive information in this new environment.

In this seminar, we will discuss:

- What is Big Data, who is using it, and how does it differ from "small" data?
- The major control, compliance, and security issues associated with the technology
- A framework for control and security over Big Data
- Use of Big Data to enhance audit, compliance, and security

Learning Objectives

- What is Big Data?
- Demystifying Big Data Mining: Hadoop, its architecture, and File System (HFS)
- Security and control issues and how they apply in Big Data environments
    - Access controls
    - Backup and recovery on a Big scale
    - Location in the Cloud: Big Data on the move and at rest, encryption, tokenization, rights management
    - Managing Big Data: cleaning, verification, reconciliation, disposal
    - Technology: inadequate security features, insecure development tools, IT's lack of experience
    - Distributed data mining
    - Data leak protection: classification and ownership of Big Data
- A framework for Big Data security, risk and threat models for big data
- Compliance: PHI, PCI-DSS, Cross-Border Privacy Rules (CBPR)
- Big Data on our side: gathering audit data; and big security data
- Developing standards: Big Data Working Group (BDWG)

Learning Level: Basic

TRACK H-2
THREAT MODELING: FINDING SECURITY THREATS BEFORE THEY HAPPEN (JEFF KALWERISKY - WEDNESDAY)
7 CPEs

Seminar Focus and Features

Threat Modeling is a methodology for documenting potential risks and vulnerabilities in information systems (applications, networks, etc.). It allows auditors and information security specialists to focus on, and document, specific classes of threats and control weaknesses together with relevant remediation or compensating controls. Using a standard form of data flow diagrams (DFDs), parts of applications to entire systems can easily be documented in a standard format which can be understood by developers, auditors, information security specialists, and management. All of this information can be stored in a database which forms an electronic trail, over the entire lifecycle (SDLC) of the application or system, of the vulnerabilities and control weaknesses inherent in the system and the corresponding resolution or corrective action. Review of the database records can then be mapped to continuous monitoring and continuous auditing processes.

In this seminar, we will discuss:

- The major classes of threats, known by the acronym, STRIDE
- Building threat surfaces for applications and systems – in production or in development
- Data flow diagrams for documenting threat surfaces
- Building a threat model – hands-on case studies
- Creating a database of the threat surface for the life of the application/system

Learning Objectives

- The differences in viewpoint between developers and security/control professionals
- Gain an understanding of threat surfaces
- Using DFDs to document threats and flaws (vulnerabilities)
- Threat trees
- Attack patterns
- Remediation of flaws
- Hands on experience of building and maintaining a database of flaws, threats, compensating controls, and remedial actions taken
- Tying Threat Models into continuous monitoring and continuous auditing processes

Prerequisites: A basic understanding of information security, IT controls, and flowcharting techniques.

Learning Level: Intermediate

About the Instructor

Jeff Kalwerisky, CA, CISA

Jeff Kalwerisky, Vice President and Director, Information Security and Technical Training at CPE Interactive, has specialized in information security, information risk management and IT auditing for over 20 years. He currently focuses on information risk, IT security governance and frameworks, and secure software development.

He has held executive positions in information security and risk management with Accenture and Booz Allen Hamilton consulting firms. In both of these capacities, he has consulted with Fortune 100 companies and national governments, assisting in their development and deployment of enterprise security governance policies and frameworks, and technology solutions that strengthen information security and data privacy/ protection. He served as infrastructure security architect on the world's largest electronic health project on behalf of the British Government's National Health Service, the world's largest electronic medical records deployment project, where he developed security governance to oversee 1,500 software architects and developers.

As manager of global security for VeriSign, he was responsible for ensuring that affiliate companies in 30 countries adhered to VeriSign's military-grade security standards appropriate to a global certification authority, which he helped to design and deploy.

Jeff was a partner with a major audit firm in South Africa and a consultant with PricewaterhouseCoopers.

He has published security and audit guides, and has developed training courses throughout the USA and internationally on a wide range of technical topics focusing on Windows security, secure e-commerce, IT auditing, cryptography and biometric security.

Jeff is originally from South Africa, where he received a Bachelor of Science in Physics and Math, a Masters of Science in Computer Science from University of Witwatersrand, Johannesburg, and Masters in Finance and Auditing from the University of South Africa, Pretoria. He is a Chartered Accountant (SA) and Certified Information Systems Auditor.

TRACK I-1
NETWORK SECURITY FUNDAMENTALS
(JOHN TANNAHILL – MONDAY)
7 CPEs

Seminar Focus and Features

This one-day session will focus on providing an understanding of TCP/IP protocols, networking and network security fundamentals. During the session, we will use a live TCP/IP network to demonstrate key concepts and tools, including firewall and IDS demonstrations.

Participants will learn:

- Understanding TP/IP Networks
  - TCP/IP Network Fundamentals
  - IP and ICMP Protocols
  - TCP/IP Application Protocols
  - IP Addressing and Domain Name Service (DNS)
  - Network Routing
  - IPEC
  - IPV6
- TCP/IP Applications
  - Understanding Security in TCP/IP Applications
  - Role of Operating System Security
  - Network Risk Assessment
  - Network Security Threats & Vulnerabilities
  - Dangerous TCP/IP Services and Top 10 vulnerabilities as they relate to TCP/IP
- Network Security Controls
  - Network Security Architecture and Design
  - Firewall and Network Segmentation Concepts
  - Security for Internet-accessible Network Segments (e.g. E-Commerce network environments)
  - Routers and Switches, including VLAN Security
  - Virtual Private Networks (VPN) Concepts
  - Remote Access and Wireless Network Security
  - IDS Concepts
  - Intrusion Response and Incident Handling
- Network Security & Audit Tools and Techniques
  - Checklist for TCP/IP Network Security Review and TCP/IP Port Scanning Tools
  - Standard Network Tools and Network Discovery Tools
  - Network Management Tools for Security and Audit Purposes
  - Information Gathering Tools and
- Security & Audit Resources
  - Security-related Web sites
  - Mailing Lists / Advisories

Learning Level: Intermediate

TRACK I-2
AUDIT & SECURITY OF WIRELESS AND MOBILE TECHNOLOGY
(JOHN TANNAHILL – TUESDAY-WEDNESDAY)
15 CPEs

Seminar Focus and Features

This two-day session will focus on the audit and security issues related to the use of wireless and mobile technologies, including detailed discussion of wireless security issues, live wireless LAN environment to demonstrate key concepts and security / audit areas, and demonstration and discussion of security and audit tools and techniques.

Specific topic areas include:

- Understanding wireless & mobile technologies
  - Wireless LANs (WLAN)
  - Wireless LAN standards and current implementations – IEEE 802.11b/g/n
  - Wi-fi protected access (WPA/WPA2)
  - Bluetooth technology and security (IEEE 802.15)
  - Other wireless technologies (e.g. Wi-Max – 802.16)
  - Mobile technologies (e.g. Blackberry, iPhone, iPad, Android, USB and removable media
- Understanding wireless and mobile technology threats and risks
  - WLAN access point security
  - War driving
  - Unauthorized network access
  - Rogue and fake access points
  - Traffic capture and analysis
  - Bluetooth threats
  - Theft / loss of client devices
- Securing and auditing wireless & mobile technologies
  - Wireless security policy and standards
  - Mobile technology security standards
  - Wireless & mobile technology risk assessment
  - Secure wireless architecture, design and deployment
  - Access point security, and authentication and encryption
  - VPN, Firewall and IS measures
  - Wireless security assessment
  - Auditing a WLAN environment
  - Wireless client security
  - Bluetooth security configuration
  - Mobile device configuration security – IOS, Android, blackberry
  - BYOD
- Security and audit tools and techniques
  - Demonstrations of wireless security and audit tools and techniques, including Kismet, Aircrack, Bluetooth Assessment tools, etc.
  - Useful reference materials

Learning Level: Intermediate

About the Instructor

John Tannahill, CA, CISM, CGEIT

John is a management consultant specializing in information security and audit services. His current focus is on information security management and control in large information systems environments and networks. His specific areas of technical expertise include UNIX and Windows operating system security, network security, and Oracle and Microsoft SQL Server security. John is a frequent speaker in Canada, Europe and the US on the subject of information security and audit. John is a member of the Toronto ISACA Chapter and has spoken at many ISACA Conferences and Chapter Events including ISACA Training Weeks; North America CACS; EuroCACS; Asia-Pacific CACS; International and Network and Information Security Conferences. John is also a 2008 Recipient of the ISACA John Kuyer Best Speaker/Best Conference Contributor.

TRACK J-1
ASSESSING YOUR PROTECTION OF PII
(JEFF KALWERISKY – MONDAY)
7 CPEs

Seminar Focus and Features

One of the unintended consequences of the information age is the availability of Personal Identifiable Information (PII). The combination of name, date of birth, and Social Security Number are the keys to the kingdom for the purposes of establishing false identity and fraud. Lost laptops, network break-ins, and phishing expeditions have led governmental entities to establish a patchwork quilt of laws requiring custodians of personal information doing business in their locality to provide safeguards and assurance that PII is secure.

In this one day seminar, we will discuss:

- PII scope and definitions
- State and Federal PII requirements
- International considerations
- Action plan for compliance

You will leave this session able to:

- Plan a risk assessment of your PII exposure
- Justify the resources needed to comply with regulatory requirements
- Identify where to focus in your evaluation of PII risk
- Integrate PII compliance into the entity-wide compliance program
- Build a PII compliance framework

Learning Level: Intermediate

TRACK J-2
AUDITING IT APPLICATION SYSTEMS
NORM KELSON – TUESDAY-WEDNESDAY)
15 CPEs

Seminar Focus and Features

Most financial application controls and processes are built into the automated functionality of the application system. In order to perform appropriate audit steps, it is necessary to understand the automated components and audit through the system. This training session prepares you to perform audits of IT-enabled application systems and provides you with the necessary technical background to understand:

- How automated applications operate
- Audit risks inherit to their design depending on application's architecture
- Identification of key transactions
- Testing methodologies

In this one day seminar, we will discuss:

- Planning the application audit
- Understanding the risks in IT Process Models
- The Key Application Processes
- Key Controls
- Audit Testing

You will also participate in group exercises and case studies.

You will leave this session able to:

- Identify IT risks in an application
- Plan and perform an automated applications review
- Perform an automated applications review
- Understand how to participate in an integrated audit of an application system

Learning Level: Basic

TRACK K
TAKING THE BULLS-EYE OFF YOUR WEBSITE: HOW TO AUDIT MODERN WEB APPLICATIONS
(KEN CUTLER, MONDAY-WEDNESDAY)
22 CPEs

Seminar Focus and Features

Increasingly demanding regulatory requirements, litigations, and intensified lethal attacks on Web-based applications, along with traditional information asset protection, have significantly raised the stakes on the importance of secure application design, testing, certification/accreditation, and audit. Additionally, IT applications have become more complex and frequently rushed to market by poorly trained commercial IT product and internal developers, increasing the business risks and the challenges to applying and verifying reliable security safeguards. In this information-packed workshop, you will cover key building blocks and significant risks, and systematically sort through the available safeguards in today's complex Web-enabled, multitiered applications. We will place special emphasis on a control point definition and transactional analysis approach to application design, security, and auditing within the context of robust, but practical enterprise architecture and governance models. Areas of emphasis include:

- Web application architectures
- HTTP state management: cookies and beyond
- Web server (Apache, IIS) security and audit
- Best practice for secure application design
- Common attacks on web applications: cross-site scripting, SQL injection, privilege escalation
- White Box and Black Box web application security testing
- Understanding the design, operation, and risks associated with Service Oriented Architectures (SOA)

Prerequisites: Auditing IT Application Systems or equivalent training. A basic understanding of IT controls and terminology is assumed.

Learning Level: Intermediate

About the Instructor

Ken Cutler, CISSP, CISA, CISM,

Ken Cutler is a Senior Teaching Fellow with CPEi, specializing in Technical Audits of IT Security and related IT controls. He is the President and Principal Consultant for Ken Cutler & Associates (KCA) InfoSec Assurance, an independent consulting firm delivering a wide array of Information Security and IT Audit management and technical professional services. He is also the Director – Q/ISP (Qualified Information Security Professional) programs for Security University. Ken Cutler was formerly Vice President of Information Security at MIS Training Institute, where his responsibilities include directing MIS Info security public training programs.

Mr. Cutler was formerly with American Express Travel Related Services where he had worldwide responsibilities for security standards, awareness programs, risk assessments, and security consulting services. Previously, he served as the CIO for Moore McCormack Resources. He also headed up the security program at Martin Marietta Data Systems.

Mr. Cutler has over 25 years of experience in information security, auditing, quality assurance, and information services. His industry experience includes insurance and financial services, natural resources, manufacturing, government contracting, consulting and training.

Mr. Cutler is the coauthor of the Commercial International Security Requirements (CISR), which offers a commercial alternative to the military security standards for system design. Mr. Cutler was a featured speaker at the 1997-2002 COMDEX conferences. He is frequently quoted in such publications as Computerworld, InfoWorld, Communications Week, and Enterprise Computing, and was featured on Talk America.

TRACK L
ADVANCED SAP
(STEVE BISKIE, MONDAY-WEDNESDAY)
22 CPEs

Seminar Focus and Features

By attending this course, you will acquire the knowledge and skills to progress beyond the basic auditing employed by many auditors and become competent at an advanced auditing level.

This 3-day course will provide you with an in-depth understanding of SAP Basis and security assessment techniques necessary for performing an in-depth technical audit and will help you take your SAP technical auditing skills to the next level. You will learn the advanced risks and control opportunities that should be considered in a thorough audit of the SAP basis system and security. On completion of this course, you will be able to: develop an effective SAP technical audit plan and prioritize key steps; discuss techniques for controlling both dialog and non-dialog user security; assess the appropriateness of SAP Basis configuration settings; recommend procedures for controlling customizations; analyze SAP Basis and security-related tables; describe effective research techniques related to advanced SAP technical issues. A live SAP system will be used for demonstration, complemented by referential screen shots, and reinforced by group discussion and class exercises.

Prerequisites: It is recommended that you have taken Audit and Security of SAP ECC and SAP R/3 or have at least an intermediate-level understanding of SAP security.

Learning Level: Advanced Field: Computer Science

About the Instructor

Steve Biskie, CISA, CITP, CPA

Steve Biskie, CISA, CITP, CPA, is the Founder of ERP Audit Solutions, a consultancy that helps organizations manage the SAP governance, audit, and control processes. He has been involved with SAP systems in a variety of roles, including as an internal auditor, consultant, implementation team member, compliance team lead, and SAP Steering Committee Chair. Mr. Biskie worked directly with SAP as part of the SAP Influence Council for the Management of Internal Controls (MIC) tool, the first iteration of what is now the SAP GRC BusinessObjects suite. Mr. Biskie was an Expert Reviewer for the 2009 publication Security, Audit, and Control Features: SAP ERP (3rd Edition), and the author of Surviving an SAP Audit (SAP Press).

REGISTRATION INFORMATION

Participation is limited. Registration will be accepted on a first-come, first-served basis. Pricing has been established to provide the maximum educational benefit for the lowest cost. Therefore, we will not be offering discounts from the established prices for early registration, membership affiliation or groups. Dress code for the conference is business casual.

Morning refreshments will be provided from 7:30 – 8:30 AM, and general sessions will be from 8:30 AM – 4:30 PM each day. Lunch will be provided. Vegetarian lunch is available via pre-registration.

Due to circumstances outside of our control, we may find it necessary to reschedule or cancel sessions or change instructors. We will give registrants advance notice of such changes, if possible.

Payment and Cancellation Policy

Please note all times are stated in Eastern Standard Time (EST). All reservations must be made online at www.isaca-det.org or www.detroitiia.org. Telephone, fax, and mail-in registrations will not be accepted.

All payments must be received by midnight 2/26/13. Payments may be made at the time of registration using Visa, MasterCard, Discover, or American Express, or check payments may be mailed to the address listed below.

Cancellations may be made online until Tuesday midnight 2/26/13 without penalty. Any cancellation received after Tuesday midnight 2/26/13 and before Monday midnight 3/4/13 will be charged a non-refundable service fee based on the CPEs of the registered course being cancelled. No refunds will be given for registrations that are cancelled after midnight 3/4/13.

CPEs	Non-Refundable Service Fee
7	$25
15	$50
22	$75

Payments (payable to: **IIA Detroit**) should be mailed to the address below. Please do not remit payment to the ISACA Detroit Chapter. Conference or registration questions should be sent to administrator@isaca-det.org.

IIA - ISACA Spring Conference
Geralyn Jarmoluk – Administrator
78850 McKay Rd
Romeo, MI 48065

Hotel Information

The spring conference committee has arranged for a discounted rate at the Doubletree Hotel Detroit/Dearborn. Register by 2/4/2013 and request the "IIA & ISACA Spring Seminar Discount" to receive a rate of $110 per room per night. The Double Tree Hotel is located at 5801 Southfield Expressway, Detroit, MI 48228. Telephone: 1-313-336-3340. Visit the IIA or ISACA web site for maps and directions.

TRACK INFORMATION

Track	Session	Dates	Fee
A-1	Outstanding Presentation and Meeting Facilitation Skills (15 CPEs)	3/11-3/12	$550
A-2	Communication and Personal Management Skills (7 CPEs)	3/13	$275
B	Forensic Analytics, Techniques and Investigation (15 CPEs)	3/11-3/12	$550
C-1	Successful Fraud Investigations – Avoiding Pitfalls, Navigating Risks, and Achieving Results (15 CPEs)	3/11-3/12	$550
C-2	Conducting Effective Fraud Risk Assessments (7 CPEs)	3/13	$275
D-1	Auditing the Business Case and Governance of Social Media (7 CPEs)	3/11	$275
D-2	IT Auditing Principles for Internal Audit (15 CPEs)	3/12-3/13	$550
E	Risk-Based Internal Audit (22 CPEs)	3/11-3/13	$825
F	Bank Internal Audit University (22 CPEs)	3/11-3/13	$995
G	Advanced Auditing for In-Charge Auditors (22 CPEs)	3/11-3/13	$825
H-1	Big Data: How to Control (Not Fight) It (7 CPEs)	3/12	$275
H-2	Threat Modeling: Finding Security Threats Before They Happen (7 CPEs)	3/13	$275
I-1	Network Security Fundamentals (7 CPEs)	3/11	$275
I-2	Audit & Security of Wireless and Mobile Technology (15 CPEs)	3/12-3/13	$550
J-1	Assessing your Protection of PII (7 CPEs)	3/11	$275
J-2	Auditing IT Application Systems (15 CPEs)	3/12-3/13	$550
K	Web Applications Audit (22 CPEs)	3/11-3/13	$825
L	Advanced SAP (22 CPEs)	3/11-3/13	$825

Conference Location

University of Michigan Dearborn - Fairlane Center North
19000 Hubbard
Dearborn MI 48126
(Park in rear lot – north end of complex)

From the West
Take I-94 East to Southfield (M-39) and exit north. Follow Southfield (North) to the Michigan Ave. (U.S. 12) exit. Stay on the Southfield Service Drive to Hubbard Drive and turn left. Follow Hubbard Drive and turn right into the Southern entrance of the UM-Dearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building.

From the East
Take I-94 West to Southfield (M-39) and exit north. Follow Southfield (North) to the Michigan Ave. (U.S. 12) exit. Stay on the Southfield Service Drive to Hubbard Drive and turn left. Follow Hubbard Drive and turn right into the Southern entrance of the UM-Dearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building.

From the South
Take Southfield (M-39) north to the Michigan Avenue exit. Stay on the Southfield Service Drive to Hubbard Drive and turn left. Follow Hubbard Drive and turn right into the Southern entrance of the UM-Dearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building.

From the North
Take Southfield (M-39) south to the Ford Road exit. Stay on the Ford Road Service Drive to Hubbard Drive and turn right. Follow Hubbard Drive and turn right into the Southern entrance of the UM-Dearborn/Fairlane Center (The marquis will reflect the following; The University of Michigan-Dearborn/Fairlane Center). Follow the entrance road to the back and turn left at the stop sign; the North Building will be located on your left hand side. Parking is directly across from the North Building