

13<sup>th</sup> ANNUAL

# IIA / ISACA Spring Conference



MARCH 5-7, 2012  
University of  
Michigan-Dearborn  
Fairlane Center



# Welcome

If you are responsible for your company's internal auditing, information systems security and integrity, Sarbanes-Oxley compliance or other regulatory matters, or simply getting back to the basics, you will want to join us for the 13<sup>th</sup> 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. The reward comes from seeing a lot of members in attendance and hearing positive feedback. The 2012 event is no exception.

A number of classes sell out each year. Don't miss out on the opportunity to network with your peers, enhance your skills, and learn about new products & services in the marketplace! With your support, we can achieve our goal of providing a local, world-class conference tailored to meet your needs. We look forward to seeing you at the Spring Conference.

**Dan Wiechec, President, Detroit IIA Chapter**

**M. Siobhan Jordan, President, Detroit ISACA Chapter**

## **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 Breakfast – Grant Thornton**

**Monday Lunch– Accretive Solutions**

**Tuesday Breakfast - Open**

**Tuesday Lunch – Experis (formerly Jefferson Wells)**

**Wednesday Breakfast – PwC**

**Wednesday Lunch – E & Y**

## SEMINAR PROGRAM

| TRACK | MON MARCH 5  | TUES MARCH 6  | WED MARCH 7  |
|-------|--|---|--|
| A     | Securing Mobile Assets and Applications<br>(Jeff Kalwerisky)                                 | Cloud Computing – Critical Security Control Issues<br>(Jeff Kalwerisky) | Planning an IT Security Strategy<br>(Peter Davis)  |
| B     | Assessing the Security of Your Application Development Shop<br>(Yen Hoe Lee)                 |   | Preparing for a Secure and Controlled IPV6 Implementation<br>(Jeff Kalwerisky)                   |
| C     | Introduction to SAP for Internal Audit and Internal Control Professionals<br>(Gary Dickhart) |   | Introduction to SAP GRC for Internal Audit and Control Professionals<br>(Gary Dickhart)          |
| D     | Risk-Based Approach to IT Infrastructure Security & Control Assessments<br>(John Tannahill)  |   | Primer on Financial Reporting and Auditing for IT Auditors<br>(Norm Kelson)                      |
| E     | Leadership Skills<br>(Sharon Lieder)   |   | Audit Evidence & Professional Judgment: How to Effectively Use Critical Thinking<br>(Phil Flora) |
| F     | Catch Me if You Can: The Art of Fraud Detection<br>(Paul Zikmund)                            |   | Investigative Interviewing Skills<br>(Paul Zikmund)  |
| G     | Risk Based Internal Auditing<br>(Greg Duckert)   |   |  |
| H     | Internal Audit University<br>(Hernan Murdock)  |   |  |
| I     | Advanced Auditing for In-Charge Auditors<br>(Kathleen Crawford)                              |   |  |
| J     | Bank and Financial Institution Fraud<br>(Denise Cicchella)                                   |   |  |
| K     | Managing Audits as a Project<br>(John Beveridge)   |   |  |

**TRACK A -1**  
**SECURING MOBILE ASSETS AND APPLICATIONS**  
**(JEFF KALWERISKY, MONDAY)**  
**7 CPEs**

**Seminar Focus and Features**

The demand grows for Production applications on laptops, tablet computers, and smartphones. Mobile devices are being used to process sensitive and mission-critical data.

Employees are moving from the corporate offices to customer sites; working in trains, planes, and automobiles using smartphones and tablet computers to access every kind of sensitive corporate data. This is a revolution that is already happening and is likely to accelerate as mobile applications confer business advantages. The benefits of mobile computing are clear.

Unsurprisingly, malware is on the move, too, with new generations of viruses, Trojans and worms targeting mobile devices as well as ubiquitous mobile services such as SMS messaging, and Bluetooth/WiFi connectivity. This seminar addresses the business advantages of mobile computing as well as the emerging issues of how to control mobile devices, protect corporate assets, and maintain compliance with relevant legislation and data privacy standards.

In this one day seminar, we will discuss the critical issues to be considered:

- Policies and governance necessary to control mobile assets
- Ensuring that mobile devices and applications meet the security triad of Confidentiality, Integrity and Availability
- Security issues related to mobile applications and their development
- Issues related to the major platforms: Apple, Blackberry, Android, Windows, Bluetooth
- Authentication, encryption, and non-repudiation
- Multi-platform mobile environments: the Mobile Enterprise Application Platform (MEAP)
- Provisioning, patching and back up in the mobile environment

**Learning Level:** Intermediate

**TRACK A -2**  
**CLOUD COMPUTING: CRITICAL SECURITY AND CONTROL**  
**ISSUES**  
**(JEFF KALWERISKY, TUESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

Cloud Computing has been described as “the ultimate form of outsourcing.” This refers to the fact that moving into the cloud allows the enterprise to outsource or rent Infrastructure, IT services, application software, or any combination of these. In other words, IT services are purchased using a linear utility model. Although the Cloud model is attractive, CIOs express near-universal concern about one issue: security, including unauthorized access to sensitive business data (by outsiders or insiders at the Cloud ISP); availability and performance; location of the data (certain sensitive data may be prohibited by law from being stored outside the enterprise’s country boundaries); ability to retrieve the data in the event of contract termination; auditability; physical security at the ISP; and more. The Cloud model uses three models each having their own security, control, and operational concerns. This seminar addresses these issues and explores how to protect the enterprise assets.

In this one day seminar, we will discuss the critical issues to be considered:

- Before the Cloud contract is signed
- For the duration of the contract
- At contract change or renegotiation
- At the end of the contractual relationship

You will leave the session with:

- The benefits and corresponding risks associated with each Cloud Computing model.
- Who should be involved in negotiating the contract with the Cloud ISP.
- Control issues to be included up-front in the contract.
- Addressing the Cloud CIAA (Confidentiality, Integrity, Availability and Accountability).
- Metrics needed to maintain control of the outsourced Cloud environment.
- The ongoing risk assessment process in a Cloud environment.

**Learning Level:** Basic

## About the Instructor

### Jeff Kalwerisky, CA, CISA

Jeff is Director of Information Security at CPEinteractive, Inc., and 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 Master's 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 A – 3**  
**PLANNING AN IT SECURITY STRATEGY**  
**(PETER DAVIS – WEDNESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

Historically, IT security was focused on physical security, preventing malware, and defending against the onslaught of spam. External security focused on firewalls and intrusion detection/prevention devices at the network level. The threat has metamorphosed into criminal attacks on the enterprise's primary assets: its sensitive business information and its operations. In response to numerous cases of enterprises losing sensitive or proprietary information – customers' or patients' personal details, credit card numbers, social security numbers, medical histories, and more – the burden of privacy laws and regulations has also mushroomed, creating major compliance issues for the IT security function.

The focus has changed from network protection at the least possible cost to the "WSJ Test" – no corporate executive wants to be on the front page of a major newspaper associated with yet another data breach or a significant operational disruption.

IT security is now on the literal front line in the never-ending struggle to prevent data leakage and operational disruption.

In this one day seminar, we will discuss:

- The real and present threats to the Enterprise with actual case studies
- What information is actually sensitive
- Why it is so difficult to know where that information is located
- The major areas to be included in a Best of Breed security strategy
- How data loss prevention has moved to the front of the bus
- Information security strategy in a Federated world
- Effective metrics to manage IT security and communicate with business management
- Making IT security a valued and proactive partner in the business

**Prerequisites:** Understanding of risk management processes and basic information security concepts.

**Learning Level:** Intermediate

## **About the Instructor**

### **Peter Davis, Senior Fellow**

Peter Davis is an experienced subject matter expert, author, and trainer. A 30-year information systems audit and security veteran, Mr. Davis' career includes positions as security administrator, security planner, consultant, and information systems auditor.

He was formerly a principal in the Information Systems Audit practice of Ernst & Young. In the public sector, Mr. Davis was Director of Information Systems Audit in the Office of the Provincial Auditor (Ontario). Mr. Davis has assisted financial, government and retail organizations in developing their IT audit framework by determining their audit universe, performing a risk assessment of the IT universe and documenting internal control questionnaires based on the risk.

Mr. Davis also is the past President and founder of the Toronto ISSA chapter, past Recording Secretary of the ISSA's International Board and past Computer Security Institute Advisory Committee member. In addition, he was a member of the international committee formed to develop Generally Accepted System Security Principles (GSSP). Mr. Davis has written or co-written 12 books including "Lean Six Sigma Secrets for the CIO," "Hacking Wireless Networks for Dummies," "Wireless Networks for Dummies," "Computer Security for Dummies," and "Securing and Controlling Cisco Routers." Peter is listed in the International Who's Who of Professionals. He is a past Editor of EDPACS, a monthly publication for security and audit professionals.

He is a frequent speaker at ISACA and IIA chapter meetings, and was a featured instructor with MIS Training Institute. He holds the following professional certifications and accreditations: CISA, CISSP, CSP, CMA, ISP, CNA, CMC, CCNA, CWNA, CISM, COBIT Foundation Certificate, ITIL Foundation Certificate and Accredited COBIT Implementation Trainer, ISSPCS, PMP, SSGB, CGEIT.

**TRACK B - 1**  
**ASSESSING THE SECURITY OF YOUR APPLICATION**  
**DEVELOPMENT SHOP**  
**(YEN HOE LEE – MONDAY - TUESDAY)**  
**15 CPEs**

**Seminar Focus and Features**

The Application Development group in any enterprise is critical to IT's mission. However, at the same time, the security risks associated with software development are legendary. We see continual examples of successful attacks on production code by intruders, exploiting known vulnerabilities, such as buffer overflows, use of non-secure code libraries, directory traversing, untested paths in the code, and more. In addition, development shops often do not have security policies related to the development process and lack tools such as code analyzers to automate the process of discovering security vulnerabilities before code is deployed into production.

Given these risks and the business risk related to software development, it is critical for an auditor to be able to understand the issues in a development shop and assess the related business risk.

This session is intended to provide auditors with the knowledge and tools to be able to assess critically the levels of security and risk inherent in a corporate software development shop.

In this seminar, we will discuss the critical issues to be considered:

- How attackers exploit vulnerabilities due to software defects
- Why network defenses are no longer enough
- Salient differences between secure and non-secure development methodologies
- The software assurance maturity model
- Software security metrics
- Security requirements in design, secure software architecture, code reviews, design analysis, code reviews, security testing, and vulnerability management

**Prerequisites:** General understanding of IT Development methodologies.

**Learning Level:** Intermediate

## **About the Instructor**

### **Yen Hoe Lee, CISSP, CSSLP, PMP**

Yen Hoe Lee has over a decade of practical and consulting experience in working with business and technical teams to review application security maturity and architecture design.

As a former Accenture Consulting Executive and Application Security Architect, he designed and developed complex solutions in information protection architecture strategy, governance and solution for Fortune 1000 companies in industrial sectors that include Travel Management, Healthcare Insurance & Managed Care, Public Service, Financial Services, Manufacturing, and Retail. He has a demonstrated track record in the mentoring, leading, and managing teams to deliver programs and influence infrastructure and application services as well as business partners.

Yen Hoe is an associate professor in application development for an online University. He is Certified Secure Software Lifecycle Professional (CSSLP), Certified Information Systems Security Professional (CISSP), and Project Management Professional (PMP).

**TRACK B - 2**  
**PREPARING FOR A SECURE AND CONTROLLED IPV6**  
**IMPLEMENTATION**  
**(JEFF KALWERISKY – WEDNESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

When the current Internet Protocol, version 4, known as IPv4, was designed in the early days of the Internet, it was intended for a relatively small number of users in academia. The resulting design allowed for a maximum of a few billion addresses and completely ignored security. The security issue has, of course, been an ongoing and very costly problem for processing confidential data. With the exponential growth in the numbers of Internet users over the past decade, we are out of IP addresses!

The Internet architects designed IPv6 to provide a virtually unlimited number of addresses; eliminate the need for Network Address Translation (NAT); strong data security and packet authentication via mandatory IPSec.

Given the lack of new IP addresses, enterprises face an imminent conversion to IPv6. This will impact every aspect of their networks, internal and external, including routers, firewalls, desktops, laptops, and mobile devices.

In this seminar, we will discuss:

- Major features of IPv6: address space, address types, packet formats, routing, DNS, Quality of Service (QoS), network renumbering, mobile IPv6
- Conversion issues
- Security risks
- Good practice policies and procedures
- A framework for a phased, secure deployment

**Prerequisites:** Detailed understanding of networking, DNS, network routing, the OSI layer, and working knowledge of network security.

**Learning Level:** Advanced

**TRACK C - 1**  
**INTRODUCTION TO SAP FOR INTERNAL AUDITORS AND**  
**INTERNAL CONTROL PROFESSIONALS**  
**(GARY DICKHART – MONDAY- TUESDAY)**  
**15 CPEs**

**Seminar Focus and Features**

Many companies are making SAP Enterprise Software the central component to manage their financial and operational business process. The primary goals promoted in many SAP business cases are the improvement of service levels and achieving budget goals through upgrades or consolidation. However, the design of the security and control components and the ability to perform control assessments are critical to a successful sustainable application. The course will introduce the concepts important to understand implementation project integration points, risks, and business process control mapping and application security components.

In this seminar, we will:

- Discuss an implementation and project overview, and identify important SAP components in your project scope.
- Identify processes and activities relating to control integration for processes and general controls (i.e. Security and Change Management).
- Describe how to identify gaps and potential solutions for filling gaps.

Learning Objectives:

- Understand the Basic Architecture and SAP components
- Identify and evaluate risks associated with an SAP implementation project
- Describe key roles and responsibilities of business, audit and IT support personnel
- Describe the process for integrating controls into the process – in Blue Print and Realization phases
- Identify alternative approaches to defining the control framework
- Identify the application security models, and their design and preferred practices
- Identify GAPS and potential solutions for security and control

**Prerequisites:** General understanding of business processes, general controls, application controls and project management principles.

**Learning Level:** Basic

**TRACK C - 2**  
**INTRODUCTION TO SAP GRC FOR INTERNAL AUDIT AND**  
**CONTROL PROFESSIONALS**  
**(GARY DICKHART – WEDNESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

Once a business implements SAP as its central component for financial and operational processes, it must address regulatory and legal compliance. The complexity of SAP and the need for an enterprise governance and risk management solution necessitates the need to have an enterprise Governance, Risk and Control (GRC) program. If properly designed, the GRC program will address multiple regulations and help automate and rationalize controls and processes to ensure compliance. This course will explain the SAP Governance Risk and Compliance portfolio and how it can be applied to streamline compliance processes throughout your enterprise. This course also provides a baseline for our more detailed sessions focusing on Access Control, Process Control, Risk Management and Global Trade Services.

In this seminar, we will:

- Introduce the SAP Enterprise Governance Risk and Compliance Portfolio of products
- Discuss organization alignment and areas of emphasis for managing Compliance Risk
- Identify practices being used to apply Access Control, Process Control, Risk Management and Global Trade Services
- Explore critical success factors for successful deployment

Learning Objectives:

- Making Compliance and Risk Management a part of your operations
- Understanding the principal modules and roles in the SAP GRC portfolio
- Alignment of key roles and responsibilities between business, audit and IT support personnel
- Deployment examples and successful practices used by other organizations

**Prerequisites:** General understanding of the SAP architecture and attending Introduction to SAP for Internal Audit and Control Professionals.

**Learning Level:** Basic

## **About the Instructor**

### **Gary Dickhart, CISA – Director, ERP Training**

Gary leads CPEinteractive's ERP training practice and is Managing Director of GM Consulting, LLC. His firm specializes in Customer Advisory Services relating to technology acquisition and deployment of Governance Risk and Compliance products.

As Vice President of SAP's Customer Advisory Office Global Team, he established and was responsible for producing preferred practices for customers and implementers of governance, risk and compliance related products. While at SAP, Gary interacted with more than 200 customers on deployment strategies for Access Control, Identity Management Integration, and Process Control and Risk Management modules. He also pioneered the first SAP application security solution, which was acquired by BindView (now a Symantec company).

He has had extensive experience from both a commercial user and supplier perspective, and provides valuable insight to both sides of the acquisition process.

Gary held senior executive positions in audit and security with J.C. Penney Company and Amerada Hess Corporation. He developed new programs, including the first automated tool for auditing computer data integrity, the first network security tool for external and internal access, and developed the first integrated IT/operational audit approach at Hess.

Gary holds an MBA from Fordham University and a Bachelor of Science degree in Accounting from Northern Colorado University. He is a Certified Information Systems Auditor.

**TRACK D-1**  
**RISK-BASED APPROACH TO IT INFRASTRUCTURE SECURITY &  
CONTROL ASSESSMENTS**  
**(JOHN TANNAHILL – MONDAY-TUESDAY)**  
**15 CPEs**

**Seminar Focus and Features**

Key information security governance controls, including a risk-based approach to design, operation, and assessment of security and controls are critical to ensuring that an organization's information assets are adequately protected to prevent compromise.

This session will discuss a risk-based approach to assessment of security and control in the following areas:

- Configuration Management Controls
- Security Configuration Standards
- Build Processes
- Patch and Change Management Processes
- Security Event Monitoring
- Vulnerability Assessment & Management
- Security Compliance Processes

**Day 1 Workshop**

1. ***IT Infrastructure Risk & Control***: Governance, framework, mapping IT infrastructure to applications & business processes, security architecture & design, risk assessment processes, compliance, and key security metrics
2. ***Security Standards and Baselines***: Key baseline security configuration standards
3. ***Security Compliance Process and Control Assessment***: Assessment methodologies, key assessment tools, reporting results to management

**Day 2 Workshop**

1. ***Virtualization Security***: VMware ESX, ESXi, vSphere & Hyper-V risk profile, key security controls and compliance tools
2. ***Operating System Security***: WIN2008, UNIX, Linux risk profile, key security controls and compliance tools
3. ***Database Security***: Oracle, SQL server 2008, and DB2-LUW risk profile, key security controls and compliance tools
4. ***Network Security***: Network perimeter, firewalls, core switches and routers risk profile, key security controls and compliance tools

**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 D-2**  
**PRIMER ON FINANCIAL REPORTING AND AUDITING FOR IT**  
**AUDITORS**  
**(NORM KELSON – WEDNESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

One of the frequent criticisms we hear of the IT audit profession from the Chief Audit Executive, CFO, and other senior management, is a lack of attention to business and financial aspects of the enterprise. All agree the IT audit community provides the necessary opportunities for skills training in the technical aspects of the audit universe. However, most systems development or enhancement projects have to do with the financial operations of the enterprise. Many IT Auditors have indicated they want an appreciation and understanding of the financial processes, but they don't want to "train to be a financial auditor."

This seminar is designed to provide an understanding of financial accounting and auditing with a scope relevant to the IT auditor's previous training and job responsibilities.

In this seminar, we will:

- Define accounting terminology: accounting definitions and lingos.
- Describe various financial statements, and understand the underlying processes in (GAAP), PCAOB AS5 financial reporting and Auditing Standards.
- Describe the accounting cycle and the closing activities.
- Discuss each of the major processing (revenue, purchasing, inventory, etc.) cycles, defining activities within each, and key issues of which the IT auditor should be aware.
- Understand the audit issues and their affect on the financial statements.
- Identify opportunities for integrated audit procedures and procedures where IT audit can take the lead.
- Identify internal control objectives and accounting principles that should be considered in a systems development project.
- Perform exercises to support the educational objectives.

**Prerequisites:** No prior financial accounting or audit knowledge required

**Learning Level:** Basic

## About the Instructor

### Norman J. Kelson, CPA, CISA, CGEIT

Norm Kelson is a 30 year veteran with extensive experience in IT assurance and governance as a consultant with a Big 4 firm and an internal audit boutique, internal audit executive, and industry advocate. He has been responsible for building and disseminating best practices to internal audit and governance stakeholders.

As President and founder of CPE Interactive, Norm specializes in IT Assurance Risk, and Governance. He is currently engaged by ISACA to write IT Audit Programs that are available as a resource to its members. He recently completed case studies for the *IT Governance Using COBIT® and VAL IT™: Student Book 2nd Edition*, and is involved in other governance related projects for ISACA and the IT Governance Institute. In addition, he provides seminars to assurance-related organizations. He was a key member of the internal audit professional practices and standards and the global information security committees.

Previously, he was Director of IT Audit for the Dutch retailer Ahold, and was responsible for IT Audit services for Stop & Shop, Giant (Maryland and Pennsylvania), Tops, and Peapod grocery chains.

Norm was Vice President of Internal Audit Services and National IT Audit Practice Director for CBIZ Harborview Partners, where he was responsible for establishing an Internal Audit/Corporate Governance practice. He was Managing Director of IT Audit and Technical Seminars for MIS Training Institute. During his 12 year tenure he was responsible for creation, and all curriculum development, of its global IT Audit training portfolio focusing on best practices in risk-based auditing.

He 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.

As a member of both the Institute of Internal Auditors (IIA) and the Information Systems Audit and Control Association (ISACA), Norm is a frequent speaker and subject matter expert at their conferences. He is a former Executive Vice President of the New England ISACA Chapter, and recipient of the John Beveridge Achievement Award, conferred by the New England Chapter of ISACA to an individual "*who has, over and beyond the norm, contributed his or her efforts to their Profession and ISACA.*"

Norm graduated from Boston University with a Bachelor of Science in Business Administration and received an MBA from the Wharton School at the University of Pennsylvania. He is a CPA, CISA (Certified Information Systems Auditor), and CGEIT (Certified in the Governance of Enterprise Information Technology).

**TRACK E-1  
LEADERSHIP SKILLS  
(SHARON LIEDER –MONDAY – TUESDAY)  
15 CPEs**

**Seminar Focus and Features**

You pride yourself on your technical skills; however, you also have good ideas to share and feel you don't know how to really influence people and make change happen. Welcome to the other side of your job, the ability to lead and influence others by communication, collaboration, and performance management skills. In this session, we will look at:

1. Differences in leadership styles between finance and non-finance professionals and how to use this information to influence and increase "buy-in."
2. How to communicate information clearly, especially technical information and data, and what results you want to see happen.
3. Using leadership styles to learn how to give constructive feedback about performance issues and changes you want them to make, and manage subordinates better in general.
4. How to use positive feedback as a means of influencing and motivating others.

**Learning Level:** All

**About the Instructor**

**Sharon Lieder**

Sharon Lieder, a JPA Associate, is a Development and Performance Consultant specializing in organizational effectiveness, leadership development and strategic planning. Sharon has extensive experience in system change projects in the private and public sector. She is an experienced executive coach skilled in a number of assessment instruments. Her facilitation skills are utilized by executive and project teams as well as Boards of Directors.

Sharon holds an MBA from UCLA and has held positions at TRW Systems, where she was involved in one of the early organizational development programs. She also headed up the staff training department at UCLA and later at UC San Diego. Her other management positions were at General Dynamics, Teledyne Ryan Aeronautical, and MOHR Development as a senior consultant.

**TRACK E-2**  
**AUDIT EVIDENCE & PROFESSIONAL JUDGEMENT: HOW TO**  
**EFFECTIVELY USE CRITICAL THINKING**  
**(PHIL FLORA –WEDNESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

One of the most difficult skills associated with auditing is determining the propriety of audit evidence; does it support the audit objective, is it enough, is it too much and inefficient, and how does professional judgment affect the quality and quantity of auditing procedures.

This session will provide the attendees with skills and techniques necessary to identify the appropriate evidence to support the audit conclusion. The tools and techniques shared will also provide attendees with approaches to guide their use of critical thinking skills to facilitate the gathering of audit evidence. Real life examples of strong and weak evidence will be provided to further the learning process.

In this seminar, we will:

- Review the importance of appropriate, sufficient and persuasive audit evidence
- Discuss the meaning and application of professional judgment
- Identify the types of evidence and discuss methods, techniques and tools to gather information to support audit objectives/results
- Provide examples of the link between methodologies and evidence gathered to support audit results
- Provide a sample of the critical thinking process
- Demonstrate how critical thinking helps improve audit evidence
- Compare and contrast auditor judgment and critical thinking skills
- Review ways to develop critical thinking to enhance the audit process
- Demonstrate how to determine that the evidence gathered is appropriate, sufficient and persuasive to support audit conclusions

**Prerequisites:** Auditors with at least 2 years' experience in order to draw upon their professional audit experience

**Learning Level:** Intermediate

## **About the Instructor**

### **Phil Flora, Senior Fellow**

Phil Flora has over 30 years of auditing and management experience in banking, cooperatives, public and cost accounting.

In his 16 years as the Chief Audit Executive (CAE) for Texas Guaranteed (TG) Phil was responsible for the maintenance/development of the Internal Audit function that included leadership, risk assessment/audit planning, communication with management/board, staff hiring/development and other administrative/operational activities. He transformed the function to enable audit coverage of the total organization. Phil also has significant experience in conducting and receiving External Quality Assessment/Peer Reviews. He has served as the mediator for a peer review dispute resolution for the State Agency Internal Audit Forum (SAIAF). In cooperation with two other CAE's he developed an Internal Audit Leadership Development Program that assisted in the development of over 30 future audit leaders.

Phil currently serves as the Chair the Institute of Internal Auditors (IIA) International Committee, and the Committee of Research & Education Advisors (CREA – formerly known as BREA). He also serves as Trustee/Vice President of Research for the IIA Research Foundation (IIARF). He has served on IIA International Committees for 10 years, Government Relations Committee (now Public Sector) and Board of Research & Education Advisors (BREA/CREA). He is an active member of the Institute of Internal Auditors (IIA) Austin Chapter and is a past President. Phil received the IIA Austin Chapter's 2006 Practitioner of the Year Award. He is also a member of the Information Systems Audit and Control Association (ISACA) and has served on the Program Committees. Phil is a member of the Association of Certified Fraud Examiners and Project Management Institute.

He has been a frequent speaker at various national, regional, state and international conferences over the past ten years. He also has provided training on numerous subjects related to internal auditing and leadership. Phil is a qualified instructor for "Practical Software and Systems Measurement (PSM): A Foundation for Objective Project Management."

Phil received a B.S. in Accounting from Virginia Commonwealth University. He is a Certified Internal Auditor (CIA), Certified Information Systems Auditor (CISA), Certified Fraud Examiner (CFE), and has a Certification in Control Self-Assessment.

**TRACK F-1**  
**CATCH ME IF YOU CAN:**  
**THE ART OF FRAUD DETECTION**  
**(PAUL E. ZIKMUND – MONDAY - TUESDAY)**  
**15 CPEs**

**Seminar Focus and Features**

The reliance upon auditors to detect red flags of fraud continues to increase. Guidance related to internal and external auditors places more emphasis on professional skepticism, use of forensic procedures, and fraud detection techniques.

This course covers the practical side of detecting red flags of fraud during the audit. Attendees will learn the art of fraud detection through lecture, case studies and in class breakout sessions designed to facilitate critical thinking skills to better detect red flags of fraud.

Attendees will develop an understanding of the following concepts:

- Elements of fraud
- Nature of why people commit fraud
- Fraud detection and deterrence
- Elements of financial statement fraud
- Asset misappropriation schemes

Topics will include:

- Overview of asset misappropriation and financial statement fraud schemes
- Designing audit programs to detect red flags of fraud
- Fraud detection and investigation techniques
- Real-life case studies
- Break-out sessions to enhance critical thinking skills

**Learning Level:** Basic

**TRACK F-2**  
**INVESTIGATIVE INTERVIEWING SKILLS FOR AUDITORS**  
**(PAUL E. ZIKMUND – WEDNESDAY)**  
**7 CPEs**

**Seminar Focus and Features**

The increase of corporate fraud has directed the attention of the government, company boards, and shareholders to the auditing profession. The passage of audit standard 5 and SAS 99 as well as internal audit standards prescribe "forensic-type" procedures to be used during audits to enhance the auditor's ability to uncover red flags for fraud.

There is continuous emphasis placed on the value of the interview process in the pursuit of fraudulent activity. Auditors are encouraged to perform a variety of analytical procedures involving interviews of key personnel. Some examples of this recommendation include the following:

- The auditor should make inquiries of management concerning knowledge of fraud or awareness of allegations of fraud.
- The auditor is urged to speak with others within the entity about the existence of fraud.
- Making oral inquiries of major customers and suppliers.
- Inquire of individuals involved in the processing of journal entries and other adjustments.

Interviewing is a forensic tool available to auditors and, when conducted effectively, can successfully uncover indicators of fraud during the audit. A successful interviewer should possess basic interviewing skills to afford themselves the opportunity to observe deceptive behavior. Auditors who are able to conduct focused discussions and alert themselves to suspicious behavior are more likely to detect fraud. Enhanced interviewing skills also aid auditors involved in investigations of fraud and/or misconduct by better positioning them to resolve such cases.

Attendees will learn the following:

1. Uncovering signs of deception
2. Properly preparing for an interview
3. Investigative interviewing skills
4. Facts about lying and why they are important to an auditor
5. Trusting your intuition

**Learning Level:** Basic

## **About the Instructor**

### **Paul E. Zikmund, CFE, CFFA, CFD**

Paul serves as Senior Director Forensic Audit at Tyco International. He is responsible for managing a global team providing fraud investigation, detection and deterrence services to help reduce and manage the Company's fraud risk. He has 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 and Certified Forensic Financial Analyst, designs and implements programs and controls to detect fraud. He manages investigations conducted in response to allegations of fraud, misconduct or abuse occurring within Tyco. Paul also leads Tyco's fraud risk assessments and fraud awareness training. His years of public and private sector experience includes the investigation of complex financial frauds, conducting forensic audit engagements and fraud risk assessments, and providing litigation support for a variety of industries.

Before joining Tyco International, Paul was Director, Litigation Support Services, at Amper Politziner & Mattia, LLP, Principal, Fraud and Forensic Services, at SolomonEdwardsGroup, LLC, and a Senior Manager, Enterprise Risk Services, at 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 in 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, a Masters of Accountancy at Auburn University, and a Masters of Business Ethics and Compliance from the New England College of Finance. 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.

Paul is a former Board member of the Philadelphia Chapter of the Association of Certified Fraud Examiners and the National Association of Certified Valuation Analysts Certified Fraud Deterrence Board.

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

**Seminar Focus and Features**

It has become abundantly clear from past corporate missteps and such pronouncements as the COSO ERM model, the recently issued GTAG on continuous auditing and risk assessment, and the IIA position paper on enterprise risk management in the UK and Ireland, that the internal audit department must align itself very closely with the business in order to assume a vital role in the overall success of the organization. In addition, increased reliance of senior management and the audit committee on the competence of the internal audit staff necessitates that IA maximize the quality and impact of all of its efforts. To fulfill all of these expectations many organizations are taking a risk-based approach to their audits.

In this intensive three-day seminar you'll see for yourself why audit functions that focus their efforts on significant risks are able to concentrate their resources on issues that drive their businesses. You will learn how to put in place a risk-based approach that is truly business oriented. You will gain an understanding of what is necessary to make your audit function totally risk based; learn tools, techniques and methodologies that will boost auditor productivity and bullet-proof audit plans; and discover how to convert the entire audit process to a risk-based approach that will take you from planning all the way through to report writing. Throughout the seminar, class exercises will allow you to hone your risk-based auditing skills. You'll leave this session with a specific understanding of what is necessary to be risk-based and how to implement this approach.

**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 H**  
**INTERNAL AUDIT UNIVERSITY**  
**(DR. HERNAN MURDOCK – MONDAY - WEDNESDAY)**  
**22 CPEs**

**Seminar Focus and Features**

In this intensive three-day seminar you will master fundamental operational auditing techniques and learn how to use a risk-based approach to enhance your audits of the Purchasing, Marketing, Human Resources, Information Technology (IT), Management, Finance/Treasury, and Accounting functions.

You will explore the objectives of major business operation areas and learn how to identify the key risks threatening them. You will find out how to make your audits more efficient and effective and how to use data analytics to gain an in-depth understanding of business processes. You will cover such critical areas as the impact of SOX, ERM, and GRC on the organization, uncovering fraud schemes that threaten business operations, and the role of IA in helping management build strong risk management and strategic planning processes. You will leave this high-impact seminar with the skills necessary to go beyond outputs and to examine the organization's ability to achieve the necessary outcomes.

**Learning Level:** Basic

**About the Instructor**

**Dr. Hernan Murdock, CIA**

Hernan Murdock is a Senior Consultant for MIS Training Institute. Before joining MIS he was the Director of Training at Control Solutions International where he oversaw the company's training and employee development program. Prior to that, he was a Senior Project Manager leading audit and consulting projects for clients in the manufacturing, transportation, high tech, education, insurance and power generation industries. Dr. Murdock also worked at Northeastern University, Arthur Andersen, Liberty Mutual and KeyCorp and has completed projects in North America, Latin America, Europe and Asia. Dr. Murdock is a lecturer at Northeastern University where he teaches management, international business and ethics. He is the author of articles on whistle blowing programs, fraud, deception and behavioral profiling and has delivered numerous invited talks and conference presentations at internal audit, academic and government functions in the United States, Latin America and Europe.

**TRACK I**  
**ADVANCED AUDITING FOR IN-CHARGE AUDITORS**  
**(KATHLEEN CRAWFORD – 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 from the unique perspective of the in-charge position. With your peers, you will review such concepts as audit program flexibility, risk assessment, priority setting during fieldwork, and effective oral and written communications of audit findings. This course covers preliminary fieldwork, audit program development, COSO, 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**

**Kathleen M. Crawford**

Kathleen Crawford is a Senior Consultant for MIS Training Institute, and President of Crawford Consulting and Communications, LLC, a firm specializing in assurance, investigative, and advisory projects for small firms without an internal audit function. Previously, Ms. Crawford was an Internal Auditor for Vinfen Corporation, where her responsibilities included assisting management in standardizing operations, developing policies and procedures, and improving processes. In addition, she investigated all suspected financial crimes, collecting evidence to ensure successful prosecution and recovery of company and client assets. Ms. Crawford trained other investigators in a methodology for detecting and documenting fraud that met the unique compliance requirements of MA Department of Health and Human Services. She began her career as a bank auditor, first with Bank of New England, then Eastern Bank, and State Street Bank. Her responsibilities in these institutions included internal audits and fraud investigations. A member of The Institute of Internal Auditors, Ms. Crawford is a past President of the Greater Boston Chapter of The IIA. She is also a member of the Association of Certified Fraud Examiners and the American Society for Training and Development. Ms. Crawford serves as Treasurer of the Board of Trustees of the Foxborough Regional Charter School and its foundation, Friends of FRCS.

**TRACK J**  
**BANK AND FINANCIAL INSTITUTION FRAUD**  
**(DENISE CICCHELLA – MONDAY - WEDNESDAY)**  
**22 CPEs**

**Seminar Focus and Features**

In this eye-opening three-day seminar you will cover in depth fraud schemes committed by employees, vendors, and customers of financial institutions, including rogue trading, embezzlement, and external frauds. In addition, you will look at such computer-assisted fraud schemes as spear phishing and network penetration. You will learn strategies and techniques you can use to identify and investigate potential perpetrators and examine internal vulnerabilities that may increase opportunities for fraud in your institution. You will explore due diligence and “know-your-client” processes and learn how to apply these concepts to mitigate risks. You will discover how data analytics can be used as both a preventive and investigative tool.

**Learning Level:** Intermediate

**About the Instructor**

**Denise Cicchella, CIA, CFE, CCA, PMP**

Denise Cicchella is the founder of Auspicium LLC, a boutique consultancy firm focused on risk management and audit services tailored to construction and facilities management. A recognized expert in construction audit, Ms. Cicchella specializes in protecting owners from overpayment of construction costs due to contractor fraud, error, or negligence. Prior to founding Auspicium, Ms. Cicchella was Director of Altran Control Solutions, where she led the construction audit practice and was responsible for training employees and developing a methodology that led to recoveries of over 7% on construction audits. Previously, Ms. Cicchella was a Senior Auditor at Met Life, specializing in fraud investigations, records management, and property and facilities management. At MetLife she played an active role in fraud investigations for broker-dealer clients, insurance schemes, and real estate. She was also instrumental in helping MetLife Bank identify operational red flags that were indicators of customer fraud. Before joining Met Life, Ms. Cicchella was a Supervisor at United Jersey Bank, assisting the internal audit department in the investigation of employee fraud. She then transitioned to the audit department, where she audited various departments and specialized in broker-dealer operations, assisting the fraud department with its investigations, and establishing preventive measures and detecting controls. The author of *Construction Audit Guide: Overview, Monitoring and Auditing*, and co-author of *Essentials of Construction Management*, Ms. Cicchella is the president of the NY/NJ chapter of the National Association of Construction Auditors and a former member of the Woman Banker’s Association.

**TRACK K**  
**MANAGING AUDITS AS A PROJECT**  
**(JOHN BEVERIDGE – MONDAY)**  
**7 CPEs**

**Seminar Focus and Features**

As auditors, we perform assessments of our IT and business project management processes for controls, effectiveness, and efficiencies. But do we practice what we preach for our audits? We have all experienced audits with a duration well over budget. Where did these audits go off-course? Good project life cycle concepts and project management are major components that ensure the timely execution of a project within scope. Audits are projects, and the same concepts can be used to assure timely completion of audits on budget within scope. Understanding the value of project management techniques to managing audits, and the importance of using critical thinking improves the audit process. This one-day seminar focuses on project management good-practices and relates them to the audit process. Using the *Closing the Loop Framework*, we will define and walk through how to build a strong well-defined audit planning and execution process.

In this one day seminar, we will discuss:

- Project management concepts for managing audits
- Effective audit reporting techniques
- Audit performance metrics

You will leave this session able to:

- Improve the audit process
- Achieve audit goals and objectives
- Deliver audits on-time, on-budget, within scope

**Learning Level:** Intermediate

## About the Instructor

**John W. Beveridge**, CGFM, CISA, CISM, CFE, CGEIT, CQA—Director, IT Audit Training

John's 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. As Massachusetts Deputy Auditor, John is currently responsible for the Information Technology Audit Division for the Massachusetts Office of the State Auditor and serves as Co-Chair of the Commonwealth's Enterprise Security Board and member of the IT Advisory Board. He has 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 Quality Assurance specialist, and Certified in the Governance of Enterprise IT.

## 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](http://www.isaca-det.org) or [www.detroitiia.org](http://www.detroitiia.org). Telephone, fax, and mail-in registrations will not be accepted.

All payments must be received by midnight 2/21/12. 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 2/21/12 without penalty. Any cancellation received after Tuesday midnight 2/21/12 and before Monday midnight 2/27/12 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 2/27/12.

| 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](mailto:administrator@isaca-det.org).

IIA - ISACA Spring Conference  
Geraldyn 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 2/3/2012 and request the “IIA & ISACA Spring Seminar Discount” to receive a rate of \$108 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   | Securing Mobile Assets and Applications (7 CPEs)  | 3/5     | \$275 |
| A-2   | Cloud Computing – Critical Security and Control Issues (7 CPEs)                           | 3/6     | \$275 |
| A-3   | Planning and IT Security Strategy (7 CPEs)  | 3/7     | \$275 |
| B-1   | Assessing the Security of Your Application Development Shop (15 CPEs)                     | 3/5-3/6 | \$550 |
| B-2   | Preparing for a Secure and Controlled IPV6 Implementation (7 CPEs)                        | 3/7     | \$275 |
| C-1   | Introduction to SAP for Internal Audit and Internal Control Professionals (15 CPEs)       | 3/5-3/6 | \$550 |
| C-2   | Introduction to SAP GRC for Internal Audit and Internal Control Professionals (7 CPEs)    | 3/7     | \$275 |
| D-1   | Risk-Based Approach to IT Infrastructure Security and Control Assessments (15 CPEs)       | 3/5-3/6 | \$550 |
| D-2   | Primer on Financial Reporting and Auditing for IT Auditors (7 CPEs)                       | 3/7     | \$275 |
| E-1   | Leadership Skills (15 CPEs)   | 3/5-3/6 | \$550 |
| E-2   | Audit Evidence & Professional Judgment: How to Effectively Use Critical Thinking (7 CPEs) | 3/7     | \$275 |
| F-1   | Catch Me if You Can: The Art of Fraud Detection (15 CPEs)                                 | 3/5-3/6 | \$550 |
| F-2   | Investigative Interviewing Skills (7 CPEs)  | 3/7     | \$275 |
| G     | Risk Based Internal Auditing (22CPEs)   | 3/5-3/7 | \$825 |
| H     | Internal Audit University (22 CPEs)   | 3/5-3/7 | \$825 |
| I     | Advanced Auditing for In-Charge Auditors (22 CPEs)  | 3/5-3/7 | \$825 |
| J     | Bank and Financial Institution Fraud (22 CPEs)  | 3/5-3/7 | \$825 |
| K     | Managing Audits as a Project (7 CPEs)   | 3/5     | \$275 |

## Conference Location

University of Michigan 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.