20TH ANNUAL
IIA and ISACA Spring Training

March 11-13, 2019
Suburban Collection Showplace
Novi, MI
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 need continuing education, you will want to join us for the 20th annual Detroit Spring Training event.

The Detroit Chapters of the IIA and ISACA are proud to co-sponsor the annual Spring Training Event. Our goal is to provide a world-class training event tailored to your needs. Each year, the Spring Training Committee offers a comprehensive series of course offerings for our members and guests. The 2019 event is no exception.

A number of classes sell out each year so register early. Don't miss this opportunity to network with your peers, enhance your skills, and learn about new products and services in the marketplace!

Class size is limited. To be fair and equitable to all, we operate on a first-come first-serve basis, and maintain a wait list for all sold out courses. Materials are only ordered for registered individuals. Therefore, registrants are required to attend the course(s) for which they registered unless they receive prior written approval from the Spring Training Chairperson. Registrants attending unauthorized classes will not be awarded continuing education credits.

We look forward to seeing you at the Spring Training event!

The 2019 Spring Training Committee
Pam Bishop, Spring Training Chairperson
Juman Doleh-Alomary
Rhoda Henderson-Fields
Richard Lowe
Jason Angelo Sist
Brian Smith
Daniel Wiechec

NETWORKING SOCIAL EVENT!

Details to be announced at a later date.
RETURNING THIS YEAR–VENDOR EXPO!

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

Contact Jason Sist at jason.sist@gmail.com for information on sponsorship opportunities.

A Special Thanks to Our 2018 Vendors
## 2019 Spring Training Program

<table>
<thead>
<tr>
<th>TRACK</th>
<th>MON MARCH 11</th>
<th>TUES MARCH 12</th>
<th>WED MARCH 13</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>How Successful People Think</td>
<td>Promoting Civility and Building Trust</td>
<td>How to be a REAL Success</td>
</tr>
<tr>
<td></td>
<td>Don Levonius</td>
<td>Don Levonius</td>
<td>Don Levonius</td>
</tr>
<tr>
<td>B</td>
<td>How to Deliver a Dynamic Presentation</td>
<td>Valuing Diversity &amp; Inclusion AND Deterring Sexual</td>
<td>Resilient Leadership</td>
</tr>
<tr>
<td></td>
<td>Keith Levick</td>
<td>Harassment</td>
<td>Keith Levick</td>
</tr>
<tr>
<td>C</td>
<td>Successful Crisis Management</td>
<td>Navigating Instances of Workplace Violence, Haras-</td>
<td>Effective Interviewing and Interrogation</td>
</tr>
<tr>
<td></td>
<td>Paul Zikmund</td>
<td>ment and Retaliation</td>
<td>Paul Zikmund</td>
</tr>
<tr>
<td>D</td>
<td>Creating and Preserving Value with COSO ERM 2017</td>
<td>Auditing Culture: Challenges and Proven Techniques</td>
<td></td>
</tr>
<tr>
<td></td>
<td>James Roth</td>
<td>James Roth</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Internal Audit University</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hernan Murdock</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>Enterprise Risk Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Greg Duckert</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td>Advanced Auditing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Peter Higgins</td>
<td></td>
</tr>
<tr>
<td></td>
<td>John Tannahill</td>
<td>John Tannahill</td>
<td>John Tannahill</td>
</tr>
<tr>
<td>I</td>
<td>Amazon Web Services (AWS) Audit &amp; Control</td>
<td></td>
<td>Introduction to IT Auditing</td>
</tr>
<tr>
<td></td>
<td>Leighton Johnson</td>
<td></td>
<td>Leighton Johnson</td>
</tr>
<tr>
<td>J</td>
<td>Cyber Security Vulnerability &amp; Penetration Testing</td>
<td></td>
<td>Intrusion Analysis and Incident Response</td>
</tr>
<tr>
<td></td>
<td>Kevin Cardwell</td>
<td></td>
<td>Kevin Cardwell</td>
</tr>
<tr>
<td>K</td>
<td>Securing &amp; Auditing Application Software Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ken Cutler</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Audit &amp; Security of SAP ERP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Steve Biskie, Josh Moench, Lucas Leaon</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Seminar Focus and Features
What single quality do successful people from all walks of life share in common? The way they think! Successful people THINK differently. According to leadership guru John C. Maxwell in his book “How Successful People Think,” when you learn to think like successful people you discover your own path to success. Change your thinking and you change your life! Through reflection, structured discussions, group activities, and other real-world applications, this program helps participants learn and apply eleven types of thinking that will change their lives!

Learning Objectives:
• Recognize the correlation between thinking and success
• Engage in big-picture thinking to increase insights and expand options
• Embrace unpopular thinking to create new ideas, paradigms, and possibilities
• Foster shared and unselfish thinking to promote collaboration and increase cooperation

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features

Incivility is like poison to an organization! Dysfunctional attitudes and behaviors undermine employee morale, engagement, productivity, retention, health, and safety. You can’t ignore incivility, so what can you do? Promote civility and build trust. Through self-assessments, structured discussions, group activities, and other real-world applications, this program helps participants recognize early warning signs, raise organizational awareness, resolve conflict, promote civility, and restore, build and sustain a culture of trust.

Learning Objectives:

• Recognize and address potential bullying, mobbing, and harassing before it escalates
• Apply conflict resolution skills to confront uncivil behavior and address false accusations
• Recognize the warning signs and consequences of distrust
• Identify characteristics that engender trust and avoid those that undermine it

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features
Success isn’t about acquiring stuff, attaining wealth, or getting to the next level. Success is a process – a lifelong strategy of building on strengths, minimizing weaknesses, and focusing on the people and points of life that are most important. Based on wisdom from leadership guru John C. Maxwell, this program includes self-assessments, structured discussions, group activities, and other real-world applications designed to help participants improve in four key areas of life: Relationships, Equipping, Attitude, and Leadership. Learning to improve in these areas will empower you to achieve REAL success!

Learning Objectives:

- Apply relationship “rules” to influence, inspire, and add value to others
- Equip others to increase your effectiveness and achieving your dreams
- Consistently demonstrate a positive attitude despite circumstances
- Develop an action plan for becoming a more effective leader

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features
The focus of this course is to teach the skills necessary to present information in a way that captures and maintains the audience’s attention. Participants learn how to identify a purpose, and build the presentation to meet that purpose. Discussion and practice of presentation development and delivery skills create a hands-on, interactive, skill-building course.

Learning Objectives:
The program offers participants the opportunity to:
• Identify benefits of a powerful presentation
• Learn ways to overcome nervousness
• Review and apply seven actions for preparing a dynamic presentation
• Learn five questions to ask to gain a better understanding of their audience
• Master ten techniques that add variety, interest, and emphasis to the presentation
• Review the effective use of visual aides
• Discover the power of the three V’s: Visual, Verbal, and Vocal
• Present an impromptu presentation using information learned
• Learn techniques for how to handle tough questions and trouble makers
• Deliver a presentation and receive feedback
• Create an action plan for future growth

Outcome:
Enhanced ability to deliver powerful presentations.

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features

Diversity and inclusion are important pieces of an organization’s business strategy. Today’s businesses are part of the larger global business community, and workplace diversity can drive both competitive advantage and personal growth. Increasing knowledge of diversity can foster greater cultural awareness as well as tap into the strengths and talents of the entire workforce. This program focuses on developing the ability to embrace diversity, and effectively assess and respond to diversity-driven situations.

Sexual Harassment prevention training is an important element of an organization’s overall human resource initiative. This training helps managers and others follow practical guidelines to prevent sexual harassment within the corporate culture, provide a safe and positive workplace, and reduce potential legal claims. This program is designed to equip managers and others with strategies and techniques for creating a culture where sexual harassment is prevented or managed according to guidelines.

This course is based upon active learning, with rich, interactive exercises, case studies, and applied experiences.

**Learning Objectives:**
At the end of this course, participants will be able to:

- Define diversity
- Identify the components of a diverse workforce
- Recognize diversity challenges
- Reflect on personal awareness of cultural diversity
- Apply a four (4) step model to effectively communicate in diversity-driven situations
- Recognize the legal definition of sexual harassment
- Differentiate between situations that satisfy the legal definition, and those that do not
- Identify reactions to sexual harassment
- Apply strategies and techniques to prevent sexual harassment
- Help employees make good choices
- Create a respectful workforce

**Outcomes:**

Enhanced diversity and inclusion strategies and techniques resulting in improved leadership skills, greater teamwork efforts, and improved workplace staffing. These abilities may help drive competitive advantage in the global business community.

Enhanced ability to create a positive, diverse workforce environment, resulting in positive relationships, fewer incidences and legal claims.

**Prerequisite:** None

**Learning Level:** Fundamental

**Field of Study:** Auditing
Seminar Focus and Features

The *Harvard Business Review* stated in a recent article: "More than education, more than experience, more than training, a person’s level of resilience will determine who succeeds and who fails." In a constantly changing workplace, resilience is defined as how well everyday job pressures are perceived and managed, and obstacles overcome. This program focuses on building skills to strengthen resiliency in the workplace.

This course is based upon active learning, with rich, interactive exercises, case studies, and applied experiences. A resiliency assessment is provided.

**Learning Objectives:**

At the end of this course, participants will be able to:

- Identify forces of enterprise-wide change, stress, and resiliency
- Master new skills and techniques to strengthen resiliency
- Recognize change as a natural force in organizations
- Assess personal resiliency quotients
- Identify reasons people resist change
- Examine five (5) features of a resilient organization
- Create a flexible, open work environment
- Effectively manage the change process

**Outcome:**

Increased personal and organizational resiliency resulting in improved ability to manage and embrace changes connected to overall business strategy.

**Prerequisite:** None

**Learning Level:** Fundamental

**Field of Study:** Auditing
Seminar Focus and Features
How does your organization manage an overall crisis? Is there a dedicated person(s) in charge of the response plan? What is considered a crisis? How do you communicate about the event? What considerations are given to social media? Many companies, both large and small, have not carefully thought through the most basic aspects of crisis management. Crisis management requires effective and efficient collaboration between many areas of the organization in response to a crisis. Companies who have not developed and exercised a successful crisis management plan and team are likely to experience difficulties during crisis response, which significantly hinders the organization’s ability to remediate and recover from the crisis.

Topics Covered
• Elements of an effective crisis management plan
• Identifying individual and functional roles and responsibilities
• Techniques to test and audit an organization’s crisis management plan
• Planning for a crisis
• Methods to remediate and recover from a crisis
• Case studies of poor and effective crisis management

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features

In light of so many recent instances of workplace violence and harassment cases employers must be better prepared and protected to help ensure the safety of employees. This course will help attendees and their employers become better informed about incidents of workplace violence, harassment and retaliation.

The course will cover elements of an effective program to reduce the risk of incidents and enable organizations to properly respond to reports or complaints. Attendees will learn the definition of what constitutes workplace violence and harassment and examples of who can engage in these types of behavior. The course also covers early warning signs that can lead to workplace violence and provides techniques and strategies to avoid and investigate instances of violence in the workplace.

Topics Covered:

- Workplace Violence and harassment prevention, detection and investigation
- Warning Signs of Workplace Violence
- Elements of an effective workplace violence and harassment program
- Effective response plans for workplace violence including an active shooter
- Elements of an effective workplace violence and harassment policy
- Best practices to de-escalate violence in your workplace
- Methods to audit the organizations programs

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features

The increase of corporate fraud during the past several years has directed the attention of the government, company boards, and shareholders to the auditing profession. Internal and external audit standards and guideline prescribe “forensic-type” procedures to be used on every audit to enhance the auditor's ability to uncover red flags for fraud, which includes effective interviewing skills.

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. Effective interrogation skills greatly enhance the auditor's or fraud examiner's ability to resolve matters of fraud and misconduct.

Topics Covered:

- Methods for uncovering signs of deception
- Steps to properly preparing for an interview
- Investigative interviewing skills
- Facts about lying why they are important to an auditor or fraud examiner

Prerequisite: None

Learning Level: Fundamental

Field of Study: Auditing
 Seminar Focus and Features

- Benefits and challenges of implementing or converting to COSO ERM 2017
- What is essential in COSO ERM 2017 and has not changed
- What has changed, improvements and potential pitfalls
- Identify some of your organization’s strengths, possible deficiencies, and what more you need to know
- Risk management issues to help your organization improve its risk management processes using the new framework
- Game plan for applying the framework to your own organization

Topics Covered:

- What’s the Same and What’s New
  ◦ Lessons from the real world: ERM in two organizations
  ◦ Why a new Framework?
  ◦ Summary of what’s changed
  ◦ Overview of the components and principles

- Governance and Culture: Principles relating to Board oversight, operating structures, culture, core values, and human capital

- Risk, Strategy, and Objective-Setting: Principles relating to business context, risk appetite, strategy-setting, and business objectives

- Performance: Principles relating to identifying, assessing and prioritizing risks, implementing risk responses, and developing a portfolio view of risk

- Review and Revision: Principles relating to assessing substantial change, reviewing risk and performance, and pursuing improvement in ERM

- Information, Communication, and Reporting: Principles relating to information and technology, communicating risk information, and reporting on risk, culture and performance
  ◦ Key points of each principle
  ◦ Illustrative examples
  ◦ Discussion of how principles are applied in participants’ organizations
  ◦ Brief self-assessment of your own organization

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features

Why Audit Culture?
- Culture is a growing concern for internal audit’s stakeholders
- What our Standards and the real world say

Challenges, Potential Pitfalls, Keys to Success
- Cultural trade-offs
- Challenges: Complexity and subjectivity of culture and resistance of key players
- Keys to success and executive workshop using a maturity model

Focus Areas
- Techniques to foster the desired culture
- Metrics that give perspective on the culture, and observable if not measure-able indicators
- A working inventory of cultural attributes

Approaches Being Used Today
- How audit departments are auditing culture: Tips for scope, execution, reporting, and staffing
- Overview of evaluation techniques being used today

Proven Audit Evaluation Techniques
- Key to success: participative auditing
- Essential principles for evaluating aspects of culture
- How audit departments evaluate aspects of culture with and without formal tools
- Bringing cultural issues into risk assessment
- Guidelines for developing and administering audit surveys and audit surveys from IIA research

Proven Entity-Wide Evaluation Techniques
- Two proven structured interview guides:
  - Anonymous – Management Interview Guide & Self-Assessment Tool
  - Anonymous – Culture of Compliance review
- Guidelines for entity-wide structured interviews
- Guidelines for developing, advising, assessing and using entity-wide surveys
- Advantages/disadvantages of each cultural evaluation technique

Reporting Cultural Issues: Guidelines and keys to success
- Audit report techniques that lower the defensiveness of local management
- Audit rating systems that include “management awareness of risk”
- Audit report comments on cultural issues: Excerpts from audit reports based on surveys and a combination of techniques

What you will gain from this seminar:
- Be exposed to the latest thinking and guidance on evaluating culture
- Learn how leading organizations from various industries are evaluating culture
- Share your techniques for evaluating culture with other attendees and get feedback from your peers and Dr. Roth
- Work through hands-on exercises in evaluating elements of culture
- Take away proven evaluation tools from world-class audit departments
- Examples of audit report comments on weaknesses in the culture

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features
In this 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, IT, Management, Finance/Treasury and Accounting functions.

Participants 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 learn the skills necessary to go beyond outputs and to examine the organization's ability to achieve the necessary outcomes.

Prerequisite: None
Learning Level: Fundamental
Field of Study: Auditing
Seminar Focus and Features

Using the Critical Management and Governance Tool for a Top-Down, Risk-Based Approach to Mitigating Risk, this intensive three-day seminar will cover alternative methods, structures and tools that can be used for establishing an ERM. You will learn how to define which aspects need to be audited and how it should be done, gain an understanding of the key qualities that an ERM should possess, and discover why they are critical. You will explore the integration of controls and business risk and find out how an oversight tool can be created that can be owned by operations and that will yield real business returns. The key historical aspects of what ERM is and where it has come from will be discussed. However, the COSO organization have redefined the ERM model as we know it from 2004 to make it a much more business centric focus. It has done away with the classic cube format and have introduced some very significant changes in what they view the future of what ERM is today and where it is going to go from here. You will leave this session thoroughly understanding what you should expect to see when you evaluate your ERM environment or what you need to know to build the ERM environment that your organization requires to be successful or to dominate your industry.

Prerequisite: Internal Audit University or equivalent experience

Learning Level: Intermediate

Field of Study: Auditing
Seminar Focus and Features

In this three-day session you will learn the elements involved in leading risk-based audits from the unique perspective of the in-charge position. With your peers you will review such concepts as audit program development and changes, performing risk assessments, setting priorities while assigning tasks, managing staff performance during fieldwork and reviewing work papers. This seminar will equip you with the techniques to communicate effectively with team members and clients, including ways to get client buy-in through the effective preparation, documentation and communication of issues and recommendations. The course provides a solid foundation on how to leverage fundamental internal audit concepts, practices, trends and focus areas to achieve quality audits. It will provide strategies on how to market and sell internal audit effectively to the client. As the liaison between the audit team and the client, the in-charge auditor has a large responsibility that requires effective planning and flawless execution of the audit plan using project management techniques appropriately.

Prerequisite: Internal Audit University or equivalent experience

Learning Level: Intermediate

Field of Study: Auditing
MOBILE TECHNOLOGY SECURITY & AUDIT
INSTRUCTOR: JOHN TANNAHILL
7 CPEs

Seminar Focus and Features
This seminar will focus on the security and audit issues related to the use of Mobile Technologies. Seminar Highlights include a detailed discussion of mobile technology security and audit areas.

Specific Topic Areas Include:
1. Understanding Mobile Technologies
   - Mobile Technologies – Apple iOS; Android
   - Communication Technologies – WLAN, Bluetooth etc.

2. Understanding Mobile Technology Threats and Risks
   - Malware
   - Security Misconfiguration
   - Vulnerabilities / Lack of Firmware Updates
   - Fake Access Points
   - Traffic Capture and Analysis
   - Bluetooth Threats
   - Theft / Loss of Devices

3. Securing & Auditing Mobile Technologies
   - Mobile Technology Security Standards
   - Mobile Technology Risk Assessment
   - Mobile Device Management
   - Mobile Application Management
   - Authentication and Encryption
   - Anti-Malware measures including Application Whitelisting
   - Bluetooth Security Configuration
   - Mobile Device Configuration Security
   - BYOD / CYOD Issues

4. Security and Audit Tools & Techniques
   - References for security and audit tools and techniques
   - References for audit programs

Prerequisite: None
Learning Level: Intermediate
Field of Study: Auditing
Seminar Focus and Features

This session will focus on the audit and security issues related to the use of Windows 2012 / 2016 Server Operating Systems. Session highlights include discussion of Windows Server architecture and security components and understanding of audit issues specific to Windows Server operating systems.

Specific Topic Areas Include:
1. Windows Server Concepts
   - Overview of Windows Server
   - Server Versions
   - Service Packs & Hotfixes
   - Build and Deployment Processes
   - Configuration Management
   - Patch Management

2. Windows Security and Control
   - Security Baselines
   - Active Directory Security
   - Forests, Trees and Domains
   - Trust Relationship Mechanisms
   - Group Policy Objects (GPO)
   - User Accounts
   - Authentication Controls
   - User Rights
   - Groups
   - Privilege Management
   - Network Share Security
   - Directory & File Permissions
   - Registry Security
   - Security Event Logs
   - Windows Services
   - Network Security

3. Auditing the Windows Server Environment
   - Auditing Domain Controllers
   - Auditing Member Servers
   - Automated Tools/Scripts for audit testing e.g. PowerShell

Prerequisite: None
Learning Level: Intermediate
Field of Study: Auditing
Seminar Focus and Features
This seminar will focus on the audit and security issues related to the use of VMware vSphere virtualization technology. Seminar highlights include a discussion of VMware Virtual Machine architecture and security components (VMware vSphere), VMware ESXi and vCenter security and control features, and audit objectives for the ESXi and vCenter environments.

Specific Topic Areas Include:
1. VM Concepts (based on VMware technology)
   - Virtual Machine Concepts
   - VMware ESXi Host Overview
   - Guest Virtual Machines
   - VMware vCenter Overview
   - Virtualization Risks

2. VMware ESXi Host Audit
   - Security Configuration Standards
   - Configuration and Patch Management
   - Security Management
   - Network and Firewall Security
   - Guest VM Security

3. VMware vCenter Audit
   - Architecture & Design
   - Security Configuration and Hardening
   - Patch Management
   - Auditing vCenter Server
   - Privilege Management
   - Security Logging and Monitoring

4. Security and Audit Tools & Techniques
   - References to Audit Tools & Scripts

Prerequisite: None
Learning Level: Intermediate
Field of Study: Auditing
Seminar Focus and Features

Amazon Web Services (AWS) is a collection of cloud-based products that enables companies to offer online services. These products range from computing, storage, networking, database, analytics, application services, management, and developer tools which constitute the backbone of today’s web-based processes. AWS enables SAP, SharePoint and Exchange to be accessible throughout the world via the Internet. Content-based systems including the education content application Blackboard used by many universities, streaming systems providing entertainment, news and advertising content, and shopping systems all rely on AWS and similar products. Security of these systems is of paramount importance.

In this one-day introductory course, you will learn:
1. Fundamental cloud computing and AWS security concepts
2. Access control and management features of AWS
3. Data encryption methods to secure sensitive data
4. The security and compliance benefits
5. Services used to maintain governance of the control environments
6. A general understanding of the AWS audit features

Topics Covered:
1. Introduction to AWS
   • Cloud computing essentials
   • AWS infrastructure
   • AWS components

2. AWS Security Services
   • Access Control
   • Access Management
   • Data Encryption
   • Governance and Monitoring

3. AWS Auditing

4. Compliance and Assurance programs

Prerequisite: A basic understanding of cloud computing and IT security controls

Learning Level: Intermediate

Field of Study: Auditing
Seminar Focus and Features

IT Auditing is an essential skill for internal auditors. To be an effective IT auditor, one needs to understand four major components of IT audit: IT Governance and Management, General IT Controls, Applications Controls, and Development Controls. This course is an introduction to these concepts and will prepare you to pursue further training in IT Audit.

This course will introduce the fundamentals of IT auditing, core drivers behind why it is a specialized area of auditing, evolution of IT assurance, and the principle objectives of IT auditing and its relationship to integrated financial or operational auditing. It will introduce the role of IT auditing and how IT audit strategies can enhance non-IT audits. We will define critical IT concepts, governance requirements, risk assessment techniques, and related auditing concepts. Attendees will be introduced to techniques for identifying operational and control requirements for IT systems, researching control objectives and related controls, evaluating control design or appropriateness, and assessing the reliability of IT audit evidence. This course will discuss:

- The IT audit universe
- Understanding the importance of the operating culture on IT control
- Understanding the relationship of controls to control objectives
- Meeting auditing standards for compliance and attaining IT audit value
- Importance of applying comprehensive audit planning techniques to achieving audit success
- Impact of outsourced IT functions

Learning Objectives:

- Gain a working understanding of IT audit concepts and practices
- Clarify the difference and importance of general versus application control audits
- Learn how to apply internal control fundamentals to the evaluation of IT system integrity, security and availability
- Gain an understanding of the operational and control objectives of the principle areas of general control
- Further your appreciation of the importance of IT in achieving organizational objectives and in providing assurance that appropriate controls are designed, implemented and in effect to attain system integrity, security and availability

Prerequisite: None

Learning Level: Fundamental

Field of Study: Auditing
Seminar Focus and Features

In this intensive hands-on course, you will learn how to detect, assess, and exploit numerous CyberSecurity vulnerabilities that stem from improper software configuration, software inconsistencies, and design flaws within an overall network infrastructure and applications. You will also examine useful methods for uncovering wired and wireless network backdoors. Working through a series of hands-on exercises, you will discover the most common CyberSecurity mistakes made by vendors, administrators, and users, and master proven tactics for thwarting them.

You will discover methods for locating and confirming frequently exploited Web and other TCP/IP application vulnerabilities. You will get proven tips on building a powerful CyberSecurity testing tool kit using both freeware and commercial tool alternatives that will let you test for frequently exploited TCP/IP network and computing platform-specific security vulnerabilities. In addition, you will review a detailed analysis of features, platform applicability, and operational considerations associated with a wide array of CyberSecurity network security testing tools for use on both Windows and Unix workstations.

Learning Objectives:

• Identify the key incremental phases and deliverables in vulnerability and penetration testing
• Understand the importance of clear definition and communication of the “Rules of Engagement” for all parties involved
• Assess the risks, strengths, and weaknesses in different categories of testing tools
• Learn how to develop and use advanced CyberAudit software techniques to increase audit coverage

Prerequisite: Familiarity with TCP/IP concepts and terminology, including the use of basic network software utilities found in Windows and/or Unix.

Learning Level: Advanced

Field of Study: Auditing
Seminar Focus and Features
Cyber-attacks are becoming an everyday occurrence. Information security specialists are having to manage their incident response and intrusion analysis to protect the organization and provide digital evidence where appropriate. This course will provide you with an understanding of the various attack characteristics, an analysis of lessons learned from recent attacks, and allow you to create your own processes for responding to attacks of your enterprise network. Participants will learn from “live” events and scenarios from actual computer incidents. Each “live” exercise will have a series of events from firewall logs to users calling the help desk, and your task will be to review the information, then using the defined incident response plan, determine what is required to be recorded, reported in the required steps, to move forward. The incidents will increase in scope and become more challenging as the workshop progresses.

Learning Objectives:
• Learn the fundamentals of intrusions
• Examine network traffic for intrusions
• Develop a systematic process for intrusion analysis
• Explore the artifacts of emerging threat attacks
• Establish an incident response lifecycle
• Create a response template for handling basic to advanced attacks
• Process “live” monitored alerts and assess the enterprise threat
• Extract sophisticated malware information from the latest types of attacks

Prerequisite: A strong background in networking, TCP/IP, Linux, and Windows

Learning Level: Intermediate

Field of Study: Auditing
Seminar Focus and Features
Ensuring a Strong System Software Foundation for Distributed Business Applications

Computerized applications are the lifeblood of modern businesses, being both an enabler and a significant risk. Effective IT security and audit programs must ensure that these business enablers operate on a solid software infrastructure foundation to minimize risks and to improve compliance with many challenging regulatory requirements. In this highly practical, hands-on seminar, we identify the major software infrastructure building block control points used to design, operate, and secure modern distributed business applications. We also pinpoint major threats, risks and industry best practice controls associated with different distributed application configuration scenarios. To reinforce the concepts presented in the class, we guide attendees through a series of practical, repeatable hands-on IT audit and security assessment exercises targeted at each of the major software infrastructure building blocks including: operating systems (Windows Server, Unix/Linux) and associated system software, web servers (Apache, Microsoft IIS), and database management systems (Microsoft SQL Server, Oracle). Attendees will also receive valuable checklists/work programs along with copious references for supportive information and audit tools.

Prerequisite: Intermediate IT Audit School or equivalent experience

Learning Level: Advanced

Field of Study: Auditing
Seminar Focus and Features
Controlling and Managing Risks in SAP R/3 and SAP ECC Systems

Participants will investigate the risks inherent in the SAP application and review some of the effective control opportunities one can configure or into the application. We will review the risks and general control opportunities provided by SAP and examine the security and basis configuration settings necessary to support a strong control environment for the rest of the system. In addition, participants will explore where SAP is going with its SAP Governance, Risk and Compliance (GRC) suite of applications, and review the auditing and monitoring changes required to move down this path. You will learn how to structure your implementation or upgrade to avoid common audit issues post “go-live.” We will delve into advanced auditing techniques supported by tools within the standard SAP application, including the Audit Information System (AIS) as well as advanced data analysis opportunities that can be provided by ACL, IDEA and, in some cases, the SAP suite itself. Attendees will leave this high-impact seminar with the know-how to assess your own system and provide recommendations for improving both SAP configuration and usage.

*NOTE: The course materials are structured around SAP ECC 6.0, however the control risk content is generally applicable to all versions of SAP R/3 back to 4.6c.*

**Prerequisite:** Basic knowledge of SAP and IT controls

**Learning Level:** Intermediate

**Field of Study:** Auditing
ABOUT THE INSTRUCTORS....

Steve Biskie, CISA, CITP, CPA, CGMA, is a Director at RSM, one of the largest accounting and consulting firms in the world. Prior to joining RSM, he was co-founder and Managing Director of High Water Advisors, a consulting firm focused on helping organizations improve governance, risk management, compliance (GRC) and audit processes. Mr. Biskie was formerly the President of ERP Audit Solutions and Customer Solutions Director at ACL Services, Ltd. First introduced to SAP in the mid-90s while working as an external auditor for Deloitte & Touche, Mr. Biskie 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. He 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 SAP Process Control), and has been an advisor to SAP for both SAP Fraud Management and SAP Audit Management. A much sought-after trainer on SAP governance, audit, and control topics, Mr. Biskie is consistently rated as a top speaker at the SAP GRC conference. Mr. Biskie was an Expert Reviewer for Security, Audit, and Control Features: SAP ERP (3rd & 4th Editions), and authored Surviving an SAP Audit.

Kevin Cardwell is an information security and IT audit professional. In addition to his training role at CPE Interactive, he is an independent consultant providing consulting services for companies throughout the world. He focuses on computer forensics and hacking courses.

He headed the team that built the U.S. Navy Network Operations and Security Center (NOSC), served as the Leading Chief of Information Security and provided consulting services throughout the world. While in this position, he created a strategy and training plan for the development of an expert team. This effort took personnel with little or no experience and build them into an expert information security team for NOSC.

Kevin is considered an authority on information security and vulnerability assessments. He is a developer, author, instructor in computer forensics and hacking courses. He is the author of the Center for Advanced Security and Training (CAST) Advanced Network Defense and Advanced Penetration Testing courses, Building Virtual Pentesting Labs for Advanced Penetration Testing, Advanced Penetration Testing for Highly Secured Environments (second edition) and Backtrack: Testing Wireless Network Security.

He has conducted technical presentations at Blackhat USA, Hacker Halted, ISSA, and TakeDownCon conferences as well as many others.

Kevin holds a bachelor of science degree in computer science from national University in California and a Master of science in software engineering from Southern Methodist University (SMU).

Ken Cutler, CISA, CISSP, CISM 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.

An internationally recognized consultant and trainer in the Information Security and IT audit fields, he is certified and has conducted courses for: Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA) and CompTIA Security+. In cooperation with Security University, he recently was featured in two full length training videos on CISSP and Security+.

Ken was formerly Vice-President of Information Security for MIS Training Institute, Chief Information Officer of Moore McCormack Resources, a Fortune 500 company. He also directed company wide IS programs for American Express Travel Related Services, Martin Marietta Data Systems, and Midlantic Banks, Inc.

Ken has been a long-time active participant in international government and industry security standards initiatives, including: The President’s Commission on Critical Infrastructure Protection, Generally Accepted System Security Principles (GSSP), Information Technology Security Evaluation Criteria (ITSEC), US Federal Criteria, and Department of Defense (DOD) Information Assurance Certification Initiative.

He is a prolific author on information security topics. His publications include: Commercial International Security Requirements (CISR), a commercial alternative to military security standards for system security design criteria, NIST SP 800-41, “Guidelines on Firewalls and Firewall Policy”, of which he was co-author, and various works on security architecture, disaster recovery planning, wireless security, vulnerability testing, firewalls, single sign-on, and the Payment Card Industry Data Security Standard (PCI DSS).
Ken Cutler continued....

He has been frequently quoted in popular trade publications, including Computerworld, Information Security Magazine, Infoworld, Information Week, CIO Bulletin, and Healthcare Information Security Newsletter, and has been interviewed in radio programs My Technology Lawyer and Talk America.

Ken received his Bachelor of Science degree in Business Administration and Computer Science degree from SUNY Empire State College.

**Greg Duckert, MBA, CRMA, CRISC, CIA, CISA, CPA, CMA, is the Founder of Virtual Governance Institute LLC and is a Senior Consultant for MIS Training Institute. Mr. Duckert is an internationally recognized expert in the field of Enterprise Risk management. He is the author of the Wiley publication Practical Enterprise Risk Management: A Business Process Approach. He is Certified in Risk Management Assurance, Certified in Risk and Information Systems Control, a Certified Public Accountant, a Certified Information Systems Auditor, and is a Certified Internal Auditor.**

Mr. Duckert was educated at the University of Wisconsin - Madison and obtained an MBA in Accounting in 1989, a BBA in Accounting in 1978, and a BA in Economics in 1971. He specializes in consulting with major organizations regarding progressive Twenty-First Century methodologies for the construction of data centric enterprise risk assessment and management models including Financial, Operational, Regulatory, and IT areas of concern that yield high business value. He also consults with his clients in all areas of ERM, as well as auditing including continuous audit / consulting platforms. Mr. Duckert is the sole developer and owner of a proprietary approach to risk assessment and management that is applied to both ERM and to enterprise risk data centric risk methodologies for Internal Auditing for organizations of all sizes. During 2012 he worked closely with the General Director - Global Automotive Audit & International Dealer Audit and the General Auditor and Chief Risk Officer of General Motors Corporation in transitioning to his proprietary audit approach known as ORCA™ (Outcome-Risk Centric Auditing). He is currently under contract with a major organization with revenues exceeding the multi-billion $ threshold to build risk based audit and ERM data centric models using his proprietary approaches. In addition, in depth hands on consulting is also performed in the areas of operational analysis and process improvement methodologies. He has developed extensive risk assessment metric inventories for evaluating risks in all organizational areas including operations, IT application systems, IT operations, regulatory and financial areas. Mr. Duckert has addressed the Permanent Undersecretary for Military Affairs of Parliament and the Defense Audit Board of the Ministry of Defense – United Kingdom on the subject matter of creating a risk based business approach to governmental oversight. He is involved in the building of or consulting on the creation of Data Centric Risk Assessment and Management models on an ongoing basis. He conducts seminars and workshops on a global basis and is a frequent speaker at conferences in his areas of expertise.

Mr. Duckert has been engaged in the professional practice of Internal Auditing and Risk Assessment and Management for over 35 years. He founded the Internal Audit function of a Fortune 500 corporation at the age of 27 and built the audit department from non-existence to a highly competent Financial, Operational, Information Technology and Regulatory audit body. He was also the General Auditor and Chief Audit Executive at two other major organizations. The audit positions were in the Manufacturing and Health Care industries. His work in Risk Assessment and Management spans virtually all key industry types.

**Peter Higgins, CIA, CRMA** is a consultant for the MIS Training Institute and principle consultant/trainer for Boston Audit Solutions Group, which specializes in audit and risk management advisory and training services.

Prior to starting Boston Audit Solutions Group, Pete spent the majority of his career as an internal auditor in financial services, including three years as VP Corporate Audit Professional Practices at State Street Bank, where he was responsible for the research, design, implementation, and continuous improvement of audit methodologies and operating standards for approximately 200 audit professionals.

Also at State Street, Peter transitioned to the 1st-Line of Defense as VP Risk and Compliance, where he led a team (20+) to provide all facets of risk, compliance and audit/examination support for multiple business lines, geographies, and approximately 1,800 employees.
Leighton Johnson, CISM, CISA, CISSP, CIFI, CRISC, CMAS, FITSP-A is an information security and IT audit professional and a Senior Fellow in CyberSecurity and IT Audit. In addition to his training role at CPE Interactive, he is CTO of ISFMT, a company focusing on computer security, forensics consulting and certification training, and cybersecurity. He is also the founder and CEO of Chimera Security, a research and development company focusing on cryptography, mobile technology, and cloud computing to create better and more secure solutions for today’s advanced users and providers.

He has over 40 years’ experience in computer security, cybersecurity, software development, communications equipment operations and maintenance, incident response, and forensic investigations. He has taught numerous cybersecurity, anti-terrorism, forensics, and risk management courses both domestically and internationally.

He previously was the Regional CIO and Senior Security Engineer for a large directorate within Lockheed Martin Information Systems and Global Solutions Company.

He is members of the CSA CloudSIRT Working Group developing the model for collaboration among cloud providers, CERT organizations, responders and users; the CSA Security-as-of-Service working group, and other cloud related working groups. He is a contributing author to the “Encyclopedia of Information Assurance” and authored “Computer Incident Response and Forensics Team Management”, and “Security Controls Evaluation, Testing, And Assessment Handbook”.

Luca Leaon, CISA is Manager, Risk Advisory Services at RSM. Lucas is an IT risk adviser, ERP risk advisory leader and national SAP and governance, risk management and compliance (GRC) champion for RSM. He has over 11 years’ experience working in IT performing IT risk management and assisting in ERP implementations. He has significant experience working in consumer products, manufacturing, healthcare, energy and public sectors. Lucas has experience working with a variety of ERP systems’ controls, including SAP, Oracle EBS, PeopleSoft and JDE. Lucas is a member of the Minnesota IIA and ISACA Chapters.

Keith Levick, Ph.D. is the CEO of Goren and Associates, Dr. Levick has over 25 years of experience in training, professional coaching, and consulting. As a psychologist, he has spent many of his clinical years in private practice. In 1987, he began to transfer his clinical expertise into the field of business management.

For the past 20 years Dr. Levick has coached managers and executives in a variety of industries in the area of personal and professional productivity, change management and interpersonal skills. He has coached many executives in their transition from the world of management into the world of leadership.

He has developed many award winning leadership training programs and workshops that are being used by Fortune 500 organizations nationwide. Some of his clients include Chrysler, GM, Daimler, Monroe Bank & Trust, MGM Detroit Grand Casino, X-Ray Industries, and many other Fortune 500 companies.

As an executive coach, Dr. Levick is a firm believer in the value of coaching. “With high impact effective coaching, people are able to remove some of the blinders to see what is possible. Coaching can help executives and leaders to discover their core habits that are working and those that are not; only then can they reach their highest potential.”
ABOUT THE INSTRUCTORS....

**Don Levonius, M.A.** is Principal Consultant, Victory Performance Consulting LLC. As a consultant, trainer, and national public speaker, Don Levonius draws on over 17 years of progressive leadership experience, including 13 years with The Disney Company and 4 years with the Institute of Internal Auditors. He taught organizational communication for the University of Central Florida, is a leadership development instructor with Valencia State College, and holds master’s degrees in human resource development and business & organizational security management. Don is also an author for the Association of Talent Development.

After years of leading security and investigations for major retail chains and Disney theme parks, Don was asked to help create and lead Disney Security Training Institute in an effort to help combat the emerging threat of terrorism following the horrific attacks in 2001. Under his leadership, Disney security training was transformed to become an international benchmark for private and public sector security organizations.

Don was later promoted to lead operations and guest service training for 23 Walt Disney World Resort hotels (25,000 guest rooms), 200 retail and dining locations, and Disney Transport (monorails, watercraft, and buses). He subsequently became a senior leader of Disney University, the company’s corporate university.

In 2009, Don left Disney, founded Victory Performance Consulting (VPC), and began providing learning solutions for a number of organizations including General Electric, NBC Universal, the Florida Attorney General’s Office and The Institute of Internal Auditors (IIA). The IIA subsequently hired Don full-time to manage and direct development of its curriculum and learning strategies and delivery of over 200 leadership development seminars annually.


**Josh Moench, CISA** is a Supervisor of Technology and Management Consulting at RSM. Josh has more than eight years of experience in SAP security and segregations of duties (SOD) and IT audit engagements. Prior to joining RSM, Josh was the SAP security and GRC lead at a global consumer products company. He also was a consultant for a large consulting company, where he served clients in a wide variety of markets, including financial services and manufacturing. Josh has regulatory experience related to IT controls with regards to SOX, COBIT and COSO. His ERP Security and Controls software experience includes SAP and GRC. Josh is a member of Minnesota ISACA Chapter.

**Dr. Hernan Murdock, CIA, CRMA** is Vice President, Audit Division 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 Arthur Andersen, Liberty Mutual and KeyCorp.

Dr. Murdock is a senior lecturer at Northeastern University where he teaches management, leadership and ethics. He is the author of *10 Key Techniques to Improve Team Productivity* and *Using Surveys in Internal Audits*, both published by the IIA Research Foundation. He has also written articles and book chapters on whistleblowing programs, international auditing, mentoring programs, fraud, deception, corporate social responsibility, and behavioral profiling. He has conducted audits and consulting projects, delivered seminars and invited talks, and made numerous presentations at internal audit, academic and government functions in North America, Latin America, Europe and Africa.
James Roth, PhD, CIA, CCSA, CRMA is president of AuditTrends, LLC, a training firm devoted to identifying and communicating the best of current internal audit practice. Jim has 35 years of progressive internal audit and teaching experience. His publications include nine AuditTrends seminars, nine books and seven other major works for the IIA International. He wrote all of the IIA’s early research studies and training programs on COSO. His publications include:

- Value-Added Business Controls: The Right Way to Manage Risk
- Control Model Implementation: Best Practices
- Internal Audit’s Role in Corporate Governance: Sarbanes-Oxley Compliance
- Four Approaches to Enterprise Risk Management
- Best Practices: Evaluating the Corporate Culture
- Adding Value with COSO 2013: Beyond Sarbanes-Oxley Compliance

In 2008 the IIA gave Jim the Bradford Cadmus Memorial Award, which was “established...to honor individuals making the greatest contribution to the advancement of the internal audit profession.” En-ergetic and motivating, Jim is one of the highest rated speakers on internal audit.

John G. Tannahill, CA, CISM, CGEIT, CRISC is an independent Information Security and Audit Services Consultant. His current consulting work areas are focused on information security in large information systems environments and networks, requiring detailed knowledge of the major operating systems encountered. Particular areas of technical security expertise include:

- Windows 2008/2012
- Unix (including Solaris, AIX & Linux)
- Oracle; Microsoft SQL Server & DB2
- Network and Firewall security

John is a frequent speaker in Canada, USA and Europe on the subject of Information Security. He is a member of the Institute of Chartered Accountants of Scotland.

Paul E. Zikmund serves as Deputy Chief Compliance Officer & VP Global Security for Bunge in White Plains, NY where he manages programs and controls designed to promote an organizational culture committed to integrity, ethical conduct, and compliance with the law. He manages and conducts investigations of compliance matters, fraud and ethics violations. Paul assists with the development and implementation of tools and techniques to mitigate enterprise fraud, security & compliance risk, manages the company’s third party risk management program, and administers compliance training and awareness programs.

Prior to joining Bunge, Paul worked as the Senior Director Forensic Audit at Tyco International in Princeton, NJ and the Director Litigation Support Services at Amper, Politziner, & Mattia, LLP, in Philadelphia, PA where he was responsible for developing, implementing, and administering fraud risk management services to Tyco and other clients. He possesses nearly 28 years of experience in this field and has effectively managed global compliance and forensic audit teams at various Fortune 500 companies.

Paul is a Certified Fraud Examiner, Certified Ethics and Compliance Management professional, and a Master Analyst in Financial Forensics. He 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 at 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 ethics, compliance, and fraud risk management. He also teaches graduate level fraud and forensic accounting, white collar crime, and auditing courses at Rider University in New Jersey, LaSalle University in Pennsylvania, and Carlow University in Pennsylvania.
REGISTRATION INFORMATION

Space is limited so registration will be accepted on a first-come, first-serve basis. Pricing has been established to provide the maximum educational benefit for the lowest cost. Therefore, we do not offer discounts from the established prices for early registration, membership affiliation or groups. Dress code for the training is business casual.

Morning refreshments will be provided from 7:30 – 8:30 AM, and sessions will be from 8:30 AM – 4:30 PM each day. Lunch will be provided daily with vegetarian options.

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 http://www.eiseverywhere.com/2019springtraining and all payments must be received by midnight Tuesday February 26, 2019. 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 midnight on Tuesday February 26, 2019 without penalty. Any cancellation received after Tuesday midnight February 26, 2019, and before Monday midnight March 4, 2019 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 March 4, 2019.

<table>
<thead>
<tr>
<th>CPEs</th>
<th>Non-Refundable Service Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>$25</td>
</tr>
<tr>
<td>15</td>
<td>$50</td>
</tr>
<tr>
<td>22</td>
<td>$75</td>
</tr>
</tbody>
</table>

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

IIA - ISACA Spring Training
Administrator
P.O. Box 99340
Troy, MI 48099

Hotel Information

Individual attendees can make reservations for the event directly with the Hyatt Place at the Suburban Collection Showplace reservations at 1-800-233-1234.

Reservations may also be made by logging on to: https://novi.place.hyatt.com/en/hotel/home.html?corp_id=G-AUD3 Use the Group Code: G-AUD3 to receive your discounted group rate of $134.00. Once the arrival and departure dates have been entered click on special rates and then enter the Group Code in the Group Code Box (make sure to include the G when entering the code).

All reservations must be accompanied by a first night room deposit, or guaranteed with a major credit card. Hotel will not hold any reservations unless secured by one of the above methods. Cancellations must be received a minimum of (72) hours prior to arrival for a full refund. Cancellations received less than (72) hours prior to arrival will forfeit one (1) night room and tax.

Reservations by attendees must be received on or before February 8, 2019
<table>
<thead>
<tr>
<th>Track</th>
<th>Session</th>
<th>Dates</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-1</td>
<td>How Successful People Think (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>A-2</td>
<td>Promoting Civility and Building Trust (7 CPEs)</td>
<td>3/12</td>
<td>$275</td>
</tr>
<tr>
<td>A-3</td>
<td>How to be a REAL Success (7 CPEs)</td>
<td>3/13</td>
<td>$275</td>
</tr>
<tr>
<td>B-1</td>
<td>How to Deliver a Dynamic Presentation (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>B-2</td>
<td>Valuing Diversity &amp; Inclusion and Deterring Sexual Harassment (7 CPEs)</td>
<td>3/12</td>
<td>$275</td>
</tr>
<tr>
<td>B-3</td>
<td>Resilient Leadership (7 CPEs)</td>
<td>3/13</td>
<td>$275</td>
</tr>
<tr>
<td>C-1</td>
<td>Successful Crisis Management (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>C-2</td>
<td>Navigating Instances of Workplace Violence, Harassment and Retaliation (7 CPEs)</td>
<td>3/12</td>
<td>$275</td>
</tr>
<tr>
<td>C-3</td>
<td>Effective interviewing and interrogation (7 CPEs)</td>
<td>3/13</td>
<td>$275</td>
</tr>
<tr>
<td>D-1</td>
<td>Creating and Preserving Value with COSO ERM 2017 (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>D-2</td>
<td>Auditing Culture: Challenges and Proven Techniques (15 CPEs)</td>
<td>3/12-3/13</td>
<td>$550</td>
</tr>
<tr>
<td>E</td>
<td>Internal Audit University (22 CPEs)</td>
<td>3/11-3/13</td>
<td>$825</td>
</tr>
<tr>
<td>F</td>
<td>Enterprise Risk Management (22 CPEs)</td>
<td>3/11-3/13</td>
<td>$825</td>
</tr>
<tr>
<td>G</td>
<td>Advanced Auditing (22 CPEs)</td>
<td>3/11-3/13</td>
<td>$825</td>
</tr>
<tr>
<td>H-1</td>
<td>Mobile Technology Security &amp; Audit (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>H-2</td>
<td>Windows Server 2012/2016 Security &amp; Audit (7 CPEs)</td>
<td>3/12</td>
<td>$275</td>
</tr>
<tr>
<td>H-3</td>
<td>VMware Security &amp; Audit (7 CPEs)</td>
<td>3/13</td>
<td>$275</td>
</tr>
<tr>
<td>I-1</td>
<td>Amazon Web Services (AWS) Audit &amp; Control (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>I-2</td>
<td>Introduction to IT Auditing (15 CPEs)</td>
<td>3/12-3/13</td>
<td>$550</td>
</tr>
<tr>
<td>J-1</td>
<td>Cyber Security Vulnerability &amp; Penetration Testing (7 CPEs)</td>
<td>3/11</td>
<td>$275</td>
</tr>
<tr>
<td>J-2</td>
<td>Intrusion Analysis and Incident Response (15 CPEs)</td>
<td>3/12-3/13</td>
<td>$550</td>
</tr>
<tr>
<td>K</td>
<td>Securing &amp; Auditing Application Software Infrastructure (22 CPEs)</td>
<td>3/11-3/13</td>
<td>$825</td>
</tr>
<tr>
<td>L</td>
<td>Audit &amp; Security of SAP ERP (22 CPEs)</td>
<td>3/11-3/13</td>
<td>$825</td>
</tr>
</tbody>
</table>
Spring Training Location

Suburban Collection Showplace
46100 Grand River Ave
Novi, MI 48374

From the West

Take I-96 East to Beck Road (exit #160), turn right and head south on Beck Road for 0.4 miles. Turn left onto Grand River Avenue and head east for .5 miles. Turn left into Suburban Collection Showplace. Park in the lot on the right as you enter the complex.

From the East

Take I-96 West to Novi Road (exit #162), turn left and head south on Novi Road. Follow Novi Road 0.4 miles to Grand River. Turn right and head west on Grand River 1.25 miles. Turn right into Suburban Collection Showplace. Park in the lot on the right as you enter the complex.