As the sun starts to set on 2019, we are excited to start setting our sights on 2020! We want to take this opportunity to reflect on another great year at MISTI, as well as to look forward to rolling out all the exciting initiatives that we have lined up for you, our valued customers, in the coming years.

MISTI has continuously delivered the very best in professional training and education for over forty years. We have made it our mission to improve both personal and business performance by equipping you with the latest skills and knowledge that you need to stay ahead. While our existing curriculum is constantly being refreshed with updated content and new classes to improve your options, during 2018 it became increasingly clear that we needed to expand the range of cybersecurity related courses that we offer in order to meet rapidly increasing customer demand.

In light of this demand, MISTI is proud to announce that in March, we acquired LeaderQuest, a business that specializes in cybersecurity certification training. LeaderQuest’s courses are actively being integrated into the 2020 MISTI offerings, enabling the single biggest expansion of our curriculum since MISTI’s inception. This is incredibly exciting for us, and we hope it is for you, too! The demands being placed on the audit team become increasingly data oriented, information security driven, and analytics related. MISTI now provides the opportunity for you to increase your knowledge in the ever-evolving area of cyber risk, together with the opportunity to prepare for and earn key cybersecurity related certifications. You can read more about LeaderQuest and these courses on pages 56 through 62 of our course catalog.

We’ve also been hard at work throughout the year enhancing our existing offerings. We have expanded courses, refined and enhanced executive programs, and increased the number of virtual classroom seminars in order to better fit your needs. Our existing seminar curricula continues to expand quickly thanks, as always, to our advisory board of principal instructors and SMEs.

In signing off, I’d also like to draw your attention to our Progression Map in this year’s catalog on the following page (page 3). The map is designed to help you personalize your training needs according to your experience level, career aspirations, and knowledge requirements. We hope that it helps you build a framework for your training needs by answering the key question: What next?

We look forward to continuing to serve your needs for the remainder of this year, next year and beyond. Everyone here at MISTI thanks you for your continued support and feedback.

Cheers,

Tony Keefe
President & CEO
MISTI
Introducing the MISTI Progression Map

What course shall I do next? What will be good for my career? These are two questions commonly asked by you, our delegates. This year, we decided to create a tool that will make it easier for you to take control of your own learning and development path.

We are delighted to share with you the MISTI Progression Map, which aligns every public MISTI seminar to one of six areas of specialty and one of four levels of experience. We have reevaluated how our courses are categorized so you can plan your learning according to your current experience, your chosen area of specialty, and your ambitions.

How does it work?

We have focused on keeping the MISTI Progression Map simple to use. Each of our courses has been assigned a Zone so that you can easily find training to suit your needs and experience level. If you are early on in your learning journey, start with Introductory level courses. If you have previously attended MISTI training, or have professional experience in a particular area, you can choose to deepen your expertise at your current level or progress to the next stage. You may be looking to develop your career in a new direction, in which case the Progression Map will assist you in broadening your expertise as you review courses outside of your current specialty.

As always, our dedicated team is standing by and ready to help guide you on your training journey, but our hope is that this tool will support you in designing your own learning plan.

We would be delighted to hear your feedback on the MISTI Progression Map. Please feel free to email us at customerservice@misti.com or call us at 508-879-7999 ext. 501 to provide your valuable input.

Thank you!
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Location</th>
<th>Start Date</th>
<th>End Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITG241</td>
<td>Advanced Auditing for In-Charge Auditors</td>
<td>NY 21-23</td>
<td>24-26</td>
<td>28-30</td>
</tr>
<tr>
<td>ITG214</td>
<td>How to Run and Deliver Successful and Timely Audits</td>
<td>OR 9-11</td>
<td>10-12</td>
<td></td>
</tr>
<tr>
<td>ITG215</td>
<td>Writing Effective Audit Reports</td>
<td>NY 14-15</td>
<td>15-16</td>
<td></td>
</tr>
<tr>
<td>ITG213</td>
<td>Auditing Corporate Culture and Ethics</td>
<td>BO 30-5/1</td>
<td>31-3/2</td>
<td></td>
</tr>
<tr>
<td>ITG250</td>
<td>CyberSecurity Audit</td>
<td>CH 7-9</td>
<td>8-10</td>
<td></td>
</tr>
<tr>
<td>ITG170</td>
<td>Fundamentals of Construction Auditing</td>
<td>NY 21-24</td>
<td>25-26</td>
<td>28-30</td>
</tr>
<tr>
<td>ITG160</td>
<td>Auditing and Controls</td>
<td>CH 18-21</td>
<td>21-22</td>
<td>23-24</td>
</tr>
<tr>
<td>ITG121</td>
<td>High-Impact Skills for Developing and Leading Your Audit Team</td>
<td>NY 14-15</td>
<td>15-16</td>
<td></td>
</tr>
<tr>
<td>ITG101</td>
<td>Successful Audit Data Analytics for Managers</td>
<td>BO 30-10/2</td>
<td>31-11/2</td>
<td></td>
</tr>
<tr>
<td>ITG902</td>
<td>Managing the Internal Audit Department</td>
<td>BO 27-29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITG800</td>
<td>Auditing Asset Management</td>
<td>NY 22-24</td>
<td>24-25</td>
<td>26-27</td>
</tr>
<tr>
<td>ITG700</td>
<td>Business Process Auditing</td>
<td>DC 6-8</td>
<td>7-9</td>
<td></td>
</tr>
<tr>
<td>ITG690</td>
<td>Building a Risk Model for Managing Functions Utilizing Business Intelligence</td>
<td>SF 2-5</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>ITG690</td>
<td>Advanced Risk-Based Internal Audit for Banks</td>
<td>MI 18-21</td>
<td>19-20</td>
<td></td>
</tr>
<tr>
<td>ITG500</td>
<td>Risk Assessing Bank Operations Using Data Analytics</td>
<td>CH 5-6</td>
<td>6-7</td>
<td></td>
</tr>
<tr>
<td>ITG425</td>
<td>ENHANCED! High-Impact Skills for Developing and Leading Your Audit Team</td>
<td>NY 14-15</td>
<td>15-16</td>
<td></td>
</tr>
<tr>
<td>ITG414</td>
<td>Mitigating Overpayment Risk and Fraud Risk in Construction Auditing</td>
<td>BO 11-13</td>
<td>12-13</td>
<td>14-15</td>
</tr>
<tr>
<td>ITG405</td>
<td>Understanding and Auditing Investments and Derivatives</td>
<td>NY 21-24</td>
<td>24-25</td>
<td>26-27</td>
</tr>
<tr>
<td>ITG390</td>
<td>Auditing Asset Management</td>
<td>NY 22-24</td>
<td>24-25</td>
<td>26-27</td>
</tr>
<tr>
<td>ITG390</td>
<td>Business Process Auditing</td>
<td>DC 6-8</td>
<td>7-9</td>
<td></td>
</tr>
<tr>
<td>ITG380</td>
<td>Building a Risk Model for Managing Functions Utilizing Business Intelligence</td>
<td>SF 2-5</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>ITG370</td>
<td>Advanced Risk-Based Internal Audit for Banks</td>
<td>MI 18-21</td>
<td>19-20</td>
<td></td>
</tr>
<tr>
<td>ITG360</td>
<td>The Audit Executive Institute</td>
<td>TRD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITG241</td>
<td>Fundamentals of Internal Auditing</td>
<td>NY 21-23</td>
<td>24-26</td>
<td>28-30</td>
</tr>
<tr>
<td>ITG214</td>
<td>How to Run and Deliver Successful and Timely Audits</td>
<td>OR 9-11</td>
<td>10-12</td>
<td></td>
</tr>
<tr>
<td>ITG215</td>
<td>Writing Effective Audit Reports</td>
<td>NY 14-15</td>
<td>15-16</td>
<td></td>
</tr>
<tr>
<td>ITG213</td>
<td>Auditing Corporate Culture and Ethics</td>
<td>BO 30-5/1</td>
<td>31-3/2</td>
<td></td>
</tr>
<tr>
<td>ITG250</td>
<td>CyberSecurity Audit</td>
<td>CH 7-9</td>
<td>8-10</td>
<td></td>
</tr>
<tr>
<td>ITG170</td>
<td>Fundamentals of Construction Auditing</td>
<td>NY 21-24</td>
<td>25-26</td>
<td>28-30</td>
</tr>
<tr>
<td>ITG160</td>
<td>Auditing and Controls</td>
<td>CH 18-21</td>
<td>21-22</td>
<td>23-24</td>
</tr>
<tr>
<td>ITG121</td>
<td>High-Impact Skills for Developing and Leading Your Audit Team</td>
<td>NY 14-15</td>
<td>15-16</td>
<td></td>
</tr>
<tr>
<td>ITG101</td>
<td>Successful Audit Data Analytics for Managers</td>
<td>BO 30-10/2</td>
<td>31-11/2</td>
<td></td>
</tr>
<tr>
<td>ITG902</td>
<td>Managing the Internal Audit Department</td>
<td>BO 27-29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITG800</td>
<td>Auditing Asset Management</td>
<td>NY 22-24</td>
<td>24-25</td>
<td>26-27</td>
</tr>
<tr>
<td>ITG700</td>
<td>Business Process Auditing</td>
<td>DC 6-8</td>
<td>7-9</td>
<td></td>
</tr>
<tr>
<td>ITG690</td>
<td>Building a Risk Model for Managing Functions Utilizing Business Intelligence</td>
<td>SF 2-5</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>ITG690</td>
<td>Advanced Risk-Based Internal Audit for Banks</td>
<td>MI 18-21</td>
<td>19-20</td>
<td></td>
</tr>
<tr>
<td>ITG500</td>
<td>Risk Assessing Bank Operations Using Data Analytics</td>
<td>CH 5-6</td>
<td>6-7</td>
<td></td>
</tr>
<tr>
<td>ITG425</td>
<td>ENHANCED! High-Impact Skills for Developing and Leading Your Audit Team</td>
<td>NY 14-15</td>
<td>15-16</td>
<td></td>
</tr>
<tr>
<td>ITG414</td>
<td>Mitigating Overpayment Risk and Fraud Risk in Construction Auditing</td>
<td>BO 11-13</td>
<td>12-13</td>
<td>14-15</td>
</tr>
<tr>
<td>ITG405</td>
<td>Understanding and Auditing Investments and Derivatives</td>
<td>NY 21-24</td>
<td>24-25</td>
<td>26-27</td>
</tr>
<tr>
<td>ITG390</td>
<td>Auditing Asset Management</td>
<td>NY 22-24</td>
<td>24-25</td>
<td>26-27</td>
</tr>
<tr>
<td>ITG390</td>
<td>Business Process Auditing</td>
<td>DC 6-8</td>
<td>7-9</td>
<td></td>
</tr>
<tr>
<td>ITG380</td>
<td>Building a Risk Model for Managing Functions Utilizing Business Intelligence</td>
<td>SF 2-5</td>
<td>3-4</td>
<td></td>
</tr>
<tr>
<td>ITG370</td>
<td>Advanced Risk-Based Internal Audit for Banks</td>
<td>MI 18-21</td>
<td>19-20</td>
<td></td>
</tr>
<tr>
<td>ITG360</td>
<td>The Audit Executive Institute</td>
<td>TRD</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Legend:**
- **Bold Dates Indicate Training Weeks**
- **Orange Dates Indicate Virtual Classroom Available**
- **NEW!** Indicates new courses for the current year.
### IT AUDIT

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Course Dates</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITA201</td>
<td>Advanced IT Audit School</td>
<td>NY 21-24</td>
<td>AT Atlanta, BU Burlington, CH Chicago</td>
</tr>
<tr>
<td>AIS231</td>
<td>Securing and Auditing Your Network Infrastructure</td>
<td>SD 7-11</td>
<td>CO Colorado Springs, DA Dallas, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS232</td>
<td>Securing and Auditing Your Application Software Infrastructure</td>
<td>SD 27-31</td>
<td>DU Denver, HH Hilton Head, HO Houston, JX Jacksonville</td>
</tr>
</tbody>
</table>

### INFORMATION SECURITY

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Course Dates</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS101</td>
<td>Introduction to Information Security</td>
<td>BO 27-29</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS203</td>
<td>Network Security Essentials</td>
<td>BO 27-29</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS207</td>
<td>Cloud Security Fundamentals</td>
<td>DC 18-20</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS151</td>
<td>Auditing Your Digital Presence</td>
<td>CH 15-16</td>
<td>NY 28-30</td>
</tr>
<tr>
<td>AIS291</td>
<td>Information Security Root Camp</td>
<td>OR 9-15</td>
<td>NY 15-19, DA Dallas, HH Hilton Head, HO Houston, JX Jacksonville</td>
</tr>
<tr>
<td>AIS370</td>
<td>NIST Cybersecurity Framework</td>
<td>NY 24-27</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS380</td>
<td>Cybersecurity Framework</td>
<td>NY 4-6</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS170</td>
<td>Security and Audit Considerations for Industrial Control Systems (ICS)</td>
<td>CH 15-18</td>
<td>NY New York, OR Orlando</td>
</tr>
<tr>
<td>AIS304</td>
<td>Comprehensive Review of Critical Security Controls</td>
<td>OR 4-6</td>
<td>DC Washington DC, NY New York</td>
</tr>
<tr>
<td>AIS391</td>
<td>Information Security Academy</td>
<td>AT 28-31</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
</tbody>
</table>

### INTEGRATED AUDIT

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Course Dates</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITA103</td>
<td>Auditing Business Application Systems</td>
<td>NY 24-25</td>
<td>AT Atlanta</td>
</tr>
<tr>
<td>AIS270</td>
<td>Assessing the Risks of Hot and Disruptive Technologies</td>
<td>SF 2-4</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS210</td>
<td>Successful Audit Data Analytics</td>
<td>NY 14-16</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS315</td>
<td>Fraud Data Analytics</td>
<td>OR 9-11</td>
<td>NY New York, OR Orlando</td>
</tr>
<tr>
<td>AIS311</td>
<td>Fraud Testing: Integrating Fraud Detection into Your Audit Program</td>
<td>SF 16-18</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS315</td>
<td>Data Mining for Auditors</td>
<td>OR 9-11</td>
<td>NY New York, OR Orlando</td>
</tr>
<tr>
<td>AIS223</td>
<td>Root Cause Analysis</td>
<td>BO 30-5/1</td>
<td>NY New York, OR Orlando</td>
</tr>
<tr>
<td>AIS211</td>
<td>Project Management for Auditors</td>
<td>SF 12-13</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>ITA212</td>
<td>Auditing Application Systems Development</td>
<td>OR 24-26</td>
<td>NY New York, OR Orlando</td>
</tr>
<tr>
<td>AIS231</td>
<td>Using Risk Assessment to Build Individual Audit Programs</td>
<td>BO 2-4</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS250</td>
<td>Building a Continuous Risk Assessment Model</td>
<td>BO 30-4/1</td>
<td>NY New York, OR Orlando</td>
</tr>
<tr>
<td>AIS401</td>
<td>How to Audit IT General Controls</td>
<td>DV 9-11</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS450</td>
<td>Audit and Security for Cloud-Based Services</td>
<td>NY 3-4</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS430</td>
<td>Securing and Auditing Windows Active Directory Domains</td>
<td>NY 21-24</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS375</td>
<td>Risk in Payment Systems</td>
<td>OR 4-7</td>
<td>MI Michigan, NY New York</td>
</tr>
<tr>
<td>AIS352</td>
<td>Governance, Risk and Compliance</td>
<td>NY 11-12</td>
<td>NY New York</td>
</tr>
<tr>
<td>AIS232</td>
<td>Managing the Fraud Audit Function</td>
<td>NY 7-9</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>ITA261</td>
<td>COBIT® 2019: Integrating COBIT into Your IT Audit Process</td>
<td>BO 30-5/1</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS361</td>
<td>Auditing the Enterprise Risk Management Process</td>
<td>NY 21-23</td>
<td>CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>AIS452</td>
<td>Audit Manager’s Guide to IT Risks</td>
<td>OR 20-21</td>
<td>SF San Francisco</td>
</tr>
</tbody>
</table>

### LEADERQUEST CERTIFICATION COURSES

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Course Dates</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>LFT181</td>
<td>ITIL Foundation Training powered by LeaderQuest</td>
<td>MLT 14-18</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>LEA101</td>
<td>CompTIA A+ Core 1 Certification Training powered by LeaderQuest</td>
<td>MLT 14-18</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>LEA201</td>
<td>CompTIA A+ Core 2 Certification Training powered by LeaderQuest</td>
<td>MLT 29-31</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>LKN201</td>
<td>CompTIA Network+ Certification Training powered by LeaderQuest</td>
<td>MLT 14-18</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>LSC301</td>
<td>CompTIA Security+ Certification Training powered by LeaderQuest</td>
<td>MLT 14-18</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
</tbody>
</table>

### ACL CERTIFIED COURSES

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Course Dates</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL101</td>
<td>A Comprehensive Introduction to ACL® Analytics</td>
<td>CH 15-19</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>ACL201</td>
<td>Functions and Case Studies within ACL® Analytics</td>
<td>CH 15-19</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
<tr>
<td>ACL303</td>
<td>Scripting with ACL® Analytics</td>
<td>CH 15-19</td>
<td>AT Atlanta, BU Burlington, CH Chicago, CO Colorado Springs, DC Washington DC, DU Dublin, OH</td>
</tr>
</tbody>
</table>
Invite MISTI to your house...

MISTI has over 40 years experience training internal auditors, IT auditors and information security professionals and has arranged over 3,000 onsite seminars for companies large and small. Let MISTI tailor a seminar for you that meets the needs and demands of your training while considering your budget constraints.

Our in-house training seminars can aid in developing the skills your staff needs to increase the productivity and quality of their work. A well-trained staff is more engaged with higher moral and initiative, which helps you retain your people. In a time of ever-changing legislative and market challenges, a well-trained staff is crucial to reduce the risks your organization will inevitably face.

Advantages of In-house training seminars

• **Save money**: If five or more people need training on the same topic, you can save 20-60% over public seminar costs by bringing a MISTI seminar in-house.

• **Save time**: Since your seminar is held at your convenience and at the location of your choice, your employees save travel costs and don’t waste valuable time away from the office.

• **Get focused and tailored content**: Choose an existing course from the MISTI catalog; combine modules for a tailored approach; or let us custom-design your course. Your training can target the most current trends and technologies affecting your organization and industry. Confidentiality is ensured, so you can tackle department hot buttons in private.

• **Engage your staff and build teamwork**: In-house participants can experience workshops, case studies, live software demonstrations, role play and hands-on computer lab exercises to address real-world solutions. Everyone hears the same message at the same time. In an in-house setting, team members also gain a greater understanding of the role each person plays in the organization.

• **Learn from the best**: All MISTI instructors are expert practitioners who are your subject-matter consultants while they are at your location. Your training is backed by MISTI’s solid industry experience and reputation. You can also take benchmarking a step further and plan a curriculum that fulfills the requirements of a MISTI Certificate Program, or design your own!

IN-HOUSE CHAPTER TRAINING

Valuable, Tailored and Convenient Training

• Bring a MISTI seminar to your professional association chapter as a cost-effective way to help your members obtain and master the knowledge and skills they need to add value to their organizations.

• Our expert faculty bring a wealth of hands-on experience and tailor the curriculum to meet the needs of your chapter.

• Our courses are designed to help your members maintain a high level of knowledge and proficiency in a wide range of fields, including internal audit, IT audit, information security management, control and governance, assurance, fraud and risk management.

• All courses offer NASBA-approved Continuing Professional Education credits (CPEs) to help your members maintain certification.

For more information, contact:
Diane Tobin, at (508) 532-3625 or dtobin@misti.com
Mimi Hatch, at (508) 532-3623 or mhatch@misti.com
MISTI Virtual Classrooms have the same world-class content and expert faculty instruction that you have come to expect, but packaged in a way that meets the demands of overloaded schedules and shrinking budgets. With the power and flexibility of a virtual platform combined with the benefits of attending in person, you don’t have to compromise your priorities to secure the training you need.

**Benefits of a MISTI Virtual Classroom include:**

- Interact with the instructor and attendees who are on site
- Reduce time away from work and home
- Save on travel and hotel costs
- Earn the same CPEs as those attending in person

MISTI’s Virtual Classrooms allow for real-time collaboration. Remote participants will interact with instructors and fellow learners as though they were physically present. Advanced audio and visual technology allows you to see and hear everything that is taking place in the classroom.

Delegates who choose to attend virtually, receive the same course materials as those attending in person. Materials will be sent directly to you prior to the class and all you need is an internet connection and webcam to participate. You will be able to raise your hand, ask questions and interact with course content. The result is an equal learning opportunity but delivered to you in whole new way.

For more information on the courses being offered in a virtual classroom please visit [www.misti.com/vtr](http://www.misti.com/vtr).

**Indicates Virtual Classroom offerings throughout the catalog**
MISTI Webinars

MISTI’s live webinars are the perfect solution for the busy professional looking for expert training. Our growing list of interactive webinars delivers NASBA certified CPE credits and is ideal for audit and information security professionals who want to stay abreast of industry trends. We recruit industry experts who bring their real-world experience to attendees and deliver practical solutions to everyday challenges.

Benefits of MISTI’s Live Webinars:
- Earn NASBA certified CPE credits
- No travel expenses or planning
- Learn from your office or home
- Affordable tuition fees
- Bring immediate value to your organization
- Access to our seasoned, experienced instructors

MISTI’s Most In-Demand Webinars:
- The Art of Cybersecurity Metrics
- Auditing Ethics in the Workplace: Tips, Tools & Techniques
- Cybersecurity: What Every Internal Auditor Needs to Know
- Developing Essential Fieldwork Skills
- Introduction to Auditing IT General Controls
- Key Elements for Audit Beginners
- Planning & Performing Integrated Audits
- Using Data Analytics Throughout the Audit Process
- Writing Audit Workpapers

Our webinar curriculum is frequently updated with new courses and dates. For a listing of our currently scheduled webinars, please visit: www.misti.com/LIVEWebinars.

Can’t attend the live session?

We know a lot of working professionals cannot always make the scheduled times of our live webinars. We’ve got you covered with recorded webinars that can be purchased and viewed independently on demand, at your own convenience!* For a listing of recorded webinars please visit: www.misti.com/RecordedWebinars.

*Note: CPE certificate credits for recorded webinars are not NASBA certified

MISTI Online Self-Study

MISTI’s Online Self-Study courses makes it possible for you to take advantage of our most popular seminar topics, earn CPEs and save on travel costs. You access courses by logging on to our online portal from your home or office and are led, at your own pace, through detailed PowerPoint presentations. Confidential exams are administered at the end of each section to allow you to test your comprehension along the way.

Online Self-Study Courses

Fundamentals of Internal Auditing: Master the concepts of traditional and operational auditing and gain proven tools and techniques for performing effective audits.
9 CPEs - Tuition: $495

IT Auditing and Controls: For those with no IT experience, this course provides a solid foundation in the basics of information systems technology as they apply to audit and security concerns and helps you prepare for the CISA* exam.
9 CPEs - Tuition: $495

Advanced Auditing for In-Charge Auditors: Explore elements involved in balancing traditional and operational risk-based auditing with the time-consuming demands of SOX compliance.
9 CPEs - Tuition: $495

Fundamentals of Information Security: This introductory course will cover the basics of information security in today’s internetworked business environment, including internal and external threats, effective security policies, contingency planning and more.
13 CPEs - Tuition: $695

Note: Online course descriptions vary from in-person seminar descriptions. For full Online Self-Study course descriptions and more information, please visit: www.misti.com/Self-Study.
**Fundamentals of Internal Auditing**

Learning the Building Blocks for Performing Effective Audits

**Seminar Focus and Features**

In this three-day seminar you will learn the concepts of internal auditing and gain proven tools and techniques to perform an effective audit. Using specifically formulated case exercises, you will examine the critical elements of internal auditing: assessing risk, flow-charting, designing flexibility into the audit program, performing the audit and applying results to solve business problems. You will get a solid background in the basics of documenting and evaluating internal control and fieldwork techniques. You will learn and put into practice the communication skills associated with internal auditing, writing audit findings and selling audit recommendations.

**Prerequisite:** None

**Advance Preparation:** None

**Field:** Auditing

**Delivery Method:** Group-Live

---

**Who Should Attend**

Internal and IT auditors with 0-3 years of experience looking for a comprehensive understanding of the process of internal audit. This foundational course can be used to onboard rotational internal auditors, and other experienced professionals starting their career in internal audit.

**What You Will Learn**

1. **Internal Audit Life Cycle and Key Concepts**
   - planning risks, stages, strategies
   - planning resources and key questions
   - stakeholder awareness
   - preliminary meetings
   - early deliverables
   - performance standards on governance

2. **Risk Assessment Strategies**
   - performance standards for risk assessment
   - different levels of risk assessment
   - key questions in risk assessment
   - balance between risk and control
   - examples of risks and risk assessment approaches

3. **Audit Project Planning**
   - performance standards on planning
   - audit equals project

4. **Documenting Internal Controls**
   - performance standards for documenting controls
   - evaluating and documenting internal controls
   - cost/benefit considerations
   - types of controls
   - the control environment
   - other barriers to good control
   - group exercises

5. **Audit Programs**
   - performance standards for audit programs
   - audit program examples
   - criteria for audit programs
   - audit objective
   - audit scope
   - audit test steps
   - sample audit program

6. **Fieldwork Techniques**
   - definitions related to evidence
   - nine fieldwork techniques
   - reliability of audit evidence
   - types of audit evidence
   - handling sensitive evidence

7. **Audit Interviews, Walkthroughs, Meetings**
   - communication overview
   - active listening
   - audit interviews and walkthroughs
   - purpose, preparation and planning
   - interview structure: five phases
   - face-to-face meetings: five reasons
   - question types
   - probing skills and questions
   - creating a work product from notes

8. **Workpapers**
   - performance standards for recording information
   - performance standards for engagement supervision
   - purposes of audit workpapers
   - workpapers completeness and accuracy
   - workpaper techniques/templates
   - electronic workpapers
   - sample workpaper
   - quality assurance and improvement programs

9. **Audit Findings**
   - attributes of audit findings
   - selling audit findings
   - template for audit findings

10. **Audit Reports and Written Communication**
    - why do auditors write reports?
    - report trends, contents, timeliness, persuasiveness
    - overview of the writing process
    - increase readability and logical flow, reduce wordiness
    - editing yourself and others

11. **Sampling and Data Analysis**
    - audit testing
    - sampling terminology
    - sampling methodologies
    - sampling for SOX compliance
    - data analysis definition, impact
    - a simple data analysis model
    - KDD process model
    - challenges in implementing data analysis

12. **Events Which Have Helped to Create Growth in Internal Audit**
    - Foreign Corrupt Practices Act
    - COSO IC-IF
    - federal sentencing guidelines
    - fraudulent financial reporting
    - blue ribbon panel
    - Sarbanes-Oxley Act
    - recent regulatory matters

---

**SCHEDULE**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Tuition</th>
<th>CPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 21-23, 2019</td>
<td>New York, NY</td>
<td>$2395</td>
<td>24</td>
</tr>
<tr>
<td>November 4-6, 2019</td>
<td>San Francisco, CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>December 9-11, 2019</td>
<td>Orlando, FL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>January 28-30, 2020</td>
<td>San Antonio, TX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>February 25-27, 2020</td>
<td>Philadelphia, PA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>March 9-11, 2020</td>
<td>San Francisco, CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>April 27-29, 2020</td>
<td>Boston, MA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>May 5-7, 2020</td>
<td>Denver, CO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>June 15-17, 2020</td>
<td>New York, NY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 13-15, 2020</td>
<td>Chicago, IL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>August 11-13, 2020</td>
<td>Atlanta, GA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>September 14-16, 2020</td>
<td>Dallas, TX</td>
<td></td>
<td></td>
</tr>
<tr>
<td>October 19-21, 2020</td>
<td>New York, NY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>November 2-4, 2020</td>
<td>San Diego, CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>December 7-9, 2020</td>
<td>Orlando, FL</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Web: misti.com/OAG101
Risk School
A Comprehensive Guide to Risk Assessment

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

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

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and external auditors; risk and compliance managers; IT auditors who require a comprehensive approach to operational audits of core business functions

What You Will Learn
1. Risk-Focused Pronouncements and Publications
2. Risk-Based Auditing
3. Risk Basics: What You Need to Know
4. Establishing a Framework for Risk Analysis
5. Aligning Key Business Risks With the Audit Universe
6. Audit Plan Creation
7. Objectively Driving the Audit Risk Assessment
8. Identifying Risk Areas of Primary Concern
9. Building an Inventory of Key Risk Metrics
10. Engagement-Level Risk Assessment
11. ERM: The New Risk Frontier
12. Reengineering the Audit Process to Make It Truly Risk-Based
13. Maximizing on Risk: Internal Audit Opportunity
14. The Audit Spectrum
15. Marketing Risk-Based Auditing

SCHEDULE
December 16-19, 2019
Orlando, FL
March 9-12, 2020
San Francisco, CA
May 18-21, 2020
Washington, DC
August 17-20, 2020
Boston, MA
December 7-10, 2020
Orlando, FL

Available In-House (page 8).

Tuition $2695 32 CPEs
Web: misti.com/OAR201

Fraud Audit School
A Comprehensive Audit Guide to Responding to the Risk of Fraud

Seminar Focus and Features
Fraud Audit School is designed to provide you with a thorough understanding of the types of fraud taking place in today’s business environment and illustrate a proven audit methodology for uncovering fraud. The course will begin with the audit and conclude with the investigation. You will learn the techniques to build effective fraud prevention and detection measures into your audit plan. You will learn how to identify the fraud scenarios, prepare a fraud risk assessment, data mine for fraud, integrate fraud detection into your audit program and minimize the fraud risk through the proper fraud internal controls. Whether responding to a whistleblower or searching for the red flags of fraud, this course will prepare you to meet today’s audit standards.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and IT auditors, external auditors, forensic accountants, corporate attorneys, risk management and information security professionals seeking an understanding of the growing risks of fraud, and how to perform a project or audit assessing for fraud.

What You Will Learn
1. Understanding How Fraud Occurs
2. Building Fraud Scenarios
3. Preparing a Business Process Fraud Risk Assessment for Audit Programs
4. Incorporating Fraud Risk Assessment Into the Audit Program
5. Integrating Fraud Testing Into Your Audit Program
6. Interviewing for Fraud in the Audit Process
7. Internal Controls and Fraud
8. Misappropriation of Assets
9. Financial Statement Fraud
10. Professional Standards
11. Fraud Investigation
12. Interviewing: Admission—Seeking and Legal Elements

SCHEDULE
November 18-21, 2019
New York, NY
May 18-21, 2020
Washington, DC
July 13-16, 2020
Chicago, IL
October 19-22, 2020
New York, NY

Available In-House (page 8).

Tuition $2695 32 CPEs
Web: misti.com/OAF201
Essential Interpersonal and Team Building Skills for Auditors
Developing the Critical Behavioral Skills of Successful Auditors

Seminar Focus and Features
An effective audit team is one where the audit team members work together cohesively and towards the same end goal. This seminar will demonstrate the essential skills of teamwork and will focus on the necessary behavioral skills including effective communication, emotional intelligence, how to deal with difficult people, enabling change and working with others. This seminar will help you to:

• Appreciate the importance of behavioral skills in the world of audit
• Understand the building blocks of effective communication
• Develop tools to improve your audit projects
• Lead review and interview sessions effectively
• Practice the skills needed to lead a meeting

• Deal with the challenges that are associated with change

The class will incorporate an interactive learning experience in a stand-alone mini project providing delegates with an experiential learning platform that features many of the attributes and challenges found in any real-life audit project. Delegates will work together in teams and compete to build a structure while coping with changing customer demands and a range of internal problems. It requires on-going fine-tuning of the process to deal with changes and surprises throughout the exercise. Throughout the simulation, delegates will learn the techniques and skills to build the team synergy needed for the audit assignments that lie ahead.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal, operational, financial, application and IT audit teams

What You Will Learn
1. What Makes an Effective Auditor
2. The Critical Interpersonal Skills for a Successful Career in Audit
3. The Importance of Critical Thinking in Decision Making
4. How Much First Impressions Matter
5. The Fundamental Elements of Effective Communication
6. Your Own Preferred Communication Style
7. How to Communicate Effectively Using Simple and Concise Language
8. Techniques for Avoiding and Anticipating Misunderstanding
9. Tools to Eliminate Communication Roadblocks
10. Common Nonverbal Cues
11. Bridging the Communication Gap to Deliver Results
12. The Fundamentals of Emotional Intelligence to Build Better Work Relationships
13. How to Establish Better Team Communications
14. Tips and Tricks for Handling Conflict

Fundamentals of Construction Auditing
The Auditors’ Essential Guide to Construction and Construction Auditing

Seminar Focus and Features
In this practical course, delegates will come to understand all relevant aspects of construction and construction auditing. Using real-world examples, delegates will review situations where monitoring and risk management would have prevented significant cost overruns. The course will provide practical tips to enable you to financially manage your construction projects by managing and mitigating risk. Throughout the program, delegates will explore and share best practices as well as techniques for overcoming common challenges.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal auditors, C-Suite executives, project managers, risk management personnel

What You Will Learn
1. Construction Basics
   • understand challenges with establishing transparency
   • discuss payment applications/benefits of using technology
   • setting the rules and learning the contract
2. Construction Contracting: Contract Types, Project Delivery Methods
   • discuss the pros, cons and risks
   • template construction contracts vs. homegrown
   • contract ambiguity and owner friendly clauses
3. Project Controls
   • best practices to manage project risks
   • evaluating and developing internal project governance procedures
   • how to store and leverage data
   • procedure documents to have in place
4. Auditing Construction Costs and Ongoing Monitoring
   • establishing criteria to evaluate multiple projects
   • discuss common project delays/risks and how to stay ahead of them
   • scoping a construction audit engagement and estimate of hours needed

Tuition $2395
24 CPEs
Web: misti.com/OAG130
Internal Audit School
Subject Matter Expertise for Today’s Essential Audit Projects

Seminar Focus and Features
In this intensive four-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. Attendees 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 internal audit 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.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and external auditors; risk and compliance managers; IT auditors who require a comprehensive approach to operational audits of core business functions.

What You Will Learn
1. Key Elements of Operational Auditing
2. Components of Operational Audits
3. Auditing the Purchasing Function
4. Auditing the Marketing and Sales Function
5. Auditing the Human Resources Function
6. Auditing the Finance, Treasury and Accounting Functions
7. Auditing Information Technology
8. Auditing Supply Chain Management
9. Auditing Management and Corporate Governance
10. The Future of Operational Auditing

SCHEDULE
October 21-24, 2019
New York, NY
March 9-12, 2020
San Francisco, CA
May 18-21, 2020
Washington, DC
August 17-20, 2020
Boston, MA
October 19-22, 2020
New York, NY

Available In-House (page 8).
Tuition $2695  32 CPEs
Web: misti.com/OAP301

Advanced Auditing for In-Charge Auditors
Contemporary Practices for Leading Risk-Based Audit Projects

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 workpapers. 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. 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: Fundamentals of Internal Auditing (OAG101) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and IT auditors with 3-7 years of experience or those responsible for overseeing the planning, fieldwork and reporting of an internal audit project.

What You Will Learn
1. Auditing Concepts: The In-Charge’s Perspective
2. The Changing Control Environment
3. Marketing and Selling Internal Audit
4. Preliminary Fieldwork and Program Development
5. Risk Assessment Strategies
6. Applying Project Management
7. Fraud Awareness
8. Effective Communications
9. High-Profile Case Studies
10. Improving Productivity
11. Best Practices in Internal Audit

SCHEDULE
October 21-23, 2019
New York, NY
December 9-11, 2019
Orlando, FL
March 9-11, 2020
San Francisco, CA
April 6-8, 2020
Boston, MA
June 15-17, 2020
New York, NY
July 13-15, 2020
Chicago, IL
October 19-21, 2020
New York, NY
December 7-9, 2020
Orlando, FL

Available In-House (page 8).
Tuition $2395  24 CPEs
Web: misti.com/OAG201
How to Run and Deliver Successful and Timely Audits
Discovering How to Productively Carry Out Audits with Effectiveness and Efficiency

Seminar Focus and Features
In this three-day seminar you will learn the process and steps necessary to ensure that the time spent on your audits is used effectively and efficiently to achieve optimal results. This seminar addresses the concepts to delivering a timely and successful audit outcome. During the course, you will:
- explore the reasons why audits fail
- identify the common and avoidable traps that result in audits overrunning their budgets and not answering key questions
- review the key components to planning and focusing the audit and how they can be managed to deliver an on-time product
- learn how to assess the audit environment to avoid surprises and how to utilize tools and methods to identify the high-risk areas
- discover how to deliver successful timely audits that add value to your organization

Engaging case studies and class exercises will be used throughout to demonstrate key concepts and put theory into practice.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Advanced Auditing for In-Charge Auditors (OAG201), or equivalent experience
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Financial, operational and IT auditors; experienced auditors who want to improve their audit product

What You Will Learn
1. Defining a Successful Audit
2. The Elements of a Successful Audit
3. Effectively Planning the Audit
4. Developing the Objective and Scope
5. Communication
6. What You Need to Know
7. Identifying and Addressing Significant Risk
8. Evaluating the Adequacy of the Control Structure
9. Focusing the Audit
10. Tools to Ensure Your Staff Are Effectively Utilized
11. Efficiencies and Time Wasters
12. Managing the Audit
13. Preliminary Findings and Reports

SCHEDULE
April 6-8, 2020
New York, NY
October 5-7, 2020
Chicago, IL
Available In-House (page 8).
Tuition $2395  24 CPEs
Web: misti.com/OAG205

Writing Effective Audit Reports
Efficiently Creating Clear, Concise and Powerful Reports

Seminar Focus and Features
Audit reports can significantly lose their effect if not written well and presented in an easy-to-read format. But getting to that beautiful report stage can be painful. This two-day course is a fresh take on stale report writing. Using real issues from companies, the class focuses on how to write effective, succinct issues and how to create reports that get noticed. Not only will managers spend less time editing reports, but auditors also learn techniques to reduce that lengthy report writing stage.

This course focuses on writing skills. It will help auditors at all levels refine their writing skills and brush up on the basics. The course provides instruction on all aspects of effective writing that applies to any audit or business-related documents. You will learn techniques for organizing information and ideas and strategies for achieving clear, concise, and complete communication. Together we’ll explore how to help one another improve writing and achieve a consistent voice in writing between all audit teams. We will look at the methods to improving communication both during and after fieldwork that contribute to an overall shorter report writing stage.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Communications and Marketing
Delivery Method: Group-Live

Who Should Attend
Audit managers, supervisors and staff who have overall, or partial, responsibility for presenting audit findings; others who need to improve writing or editing skills will also benefit from this session.

What You Will Learn
1. Common Report Writing
   • writing and communication challenges
   • audience consideration
   • using your time effectively
2. Organizing Writing
   • presentation roadmap
   • how and when to use an AIR worksheet
   • AIR: 5-step formula
3. Editing
   • how the audience reads the issue
   • concise issue writing
   • ordered vs. unordered lists
   • active vs. passive voice
   • negative wording
4. Advanced Editing
   • confusing words
   • transitions
   • ratiocination
5. Email Tips
   • timing
   • audience considerations
   • dos and don’ts
6. Tone in Writing
   • connotations of words
   • placement/sequence of negation
   • relative information
   • how to change tone
   • ratiocination cleanup
7. Design Elements
   • graphics & fonts
   • layering
   • using sidelines & flow
   • executive summary
8. Audit Writing Toolbox

SCHEDULE
December 12-13, 2019
Orlando, FL
Available In-House (page 8).
Tuition $1995  16 CPEs
Web: misti.com/OAG111
Auditing Corporate Culture and Ethics
Assessing the Impacts of Culture and Ethics on an Organization

Seminar Focus and Features
More and more organizations are finding themselves in the news because of corporate failures, fraudulent events and other negative social realities. More executive management teams, Board of Directors and even regulators are realizing the linkage between corporate culture and negative events and are paying more attention to the impact culture has in an organization. This comprehensive two-day seminar provides you with the needed background, support, tools and techniques to provide the needed guidance to the Board to protect the business. While culture and ethics could be a soft area to assess, we have a former Chief Compliance and Ethics Officer to take you through every aspect and help you build a comprehensive and dynamic audit approach.

This seminar will help you to understand and connect the key components of culture and ethics; outline what is important to the Board and executive management; analyze those organizations that know what it takes to establish a great culture; the models you should consider; how to define and measure culture and ethics; discuss the need for a formal ethics committee; and then in a workshop, we will facilitate and build a comprehensive and dynamic culture and ethics audit approach for your organization.

Prerequisite: Fundamentals of Internal Audit (OAG101), Advanced In-Charge Auditing (OAG201) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
CAEs and internal audit leaders considering proposing or performing work involving corporate culture; internal auditors of all levels responsible for auditing corporate culture or auditing ethics; those looking to identify and understand processes and metrics that are most likely to indicate a positive or negative corporate culture.

What You Will Learn
1. Understanding and Connecting the Key Components of Culture and Ethics
2. What is Important to the Board and Executive Management
3. The Great, The Good, The Bad and The Ugly
4. Models to Consider—Gathering Culture & Ethics Guidance for Testing
5. Defining and Measuring Culture and Ethics—It’s a Big Job!
6. The Ethics Committee—The Need for One Today!
7. Building a Comprehensive & Dynamic Culture and Ethics Audit Approach—Workshop
8. Summary and Wrap-Up

Available In-House (page 8).
Tuition $1995 16 CPEs
Web: misti.com/OAM223

Auditing and Collaborating with Corporate Compliance
Assessing the Value Drivers and Measuring the Effectiveness of the Corporate Compliance Function

Seminar Focus and Features
This comprehensive three-day seminar will give you the building blocks to develop and measure your compliance function and enable you to conduct a thorough review and audit of the corporate compliance function. You will learn how to assess compliance in various regulatory areas, how to use value drivers and how to ensure you understand and are meeting the expectations of your Board and executive team.

This session will prepare you with what it takes to be successful in today’s highly regulated and dynamic environment. Your internal audit group will also learn how to build a best-in-class teaming relationship with the compliance function. Compliance is an area where a true teaming approach can add significant value and maximize the oversight needed in this important area.

In a workshop format, delegates will go through all the aspects needed to build a comprehensive compliance audit approach for your organization including the use of real-life case studies to determine how you would address a particular compliance situation.

Prerequisite: Fundamentals of Internal Audit (OAG101), IT Audit School (ITG121) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
CAEs, directors and managers, and all levels responsible for executing a corporate compliance review. Chief Compliance Officers and others with responsibility for compliance and risk management.

What You Will Learn
1. State of Compliance
2. The Board’s View of Compliance Activities
3. Understanding the Big Picture
4. Driving Real Value in the “Three Lines of Defense”
5. The Compliance Committee
7. The Regulatory Agency Audit and Dealing with Regulatory Agencies
8. The Hottest Regulatory Risk Areas Facing Your Business
9. Workshop: Build Your Comprehensive Audit Program for the Compliance Function
10. Case Studies—What Would You Do?
11. Final Actions and Next Steps

Tuition $2395 24 CPEs
Web: misti.com/OAP250

SCHEDULE
December 9-11, 2019
Orlando, FL
May 18-20, 2020
New York, NY
September 21-23, 2020
Orlando, FL
Available In-House (page 8).
Innovation in Internal Audit: Part 1
Innovating the Audit Process Towards Better Business Outcomes

Seminar Focus and Features
The amount, speed and impact of change has accelerated significantly, and all indicators point to more change in the future. Organizations are expected to innovate and become creative in the pursuit of business objectives, the management of risks and the implementation of appropriate controls that increase the likelihood of success in the short and longer terms. Internal auditors must understand the dynamics driving these changes, how innovation is being used in modern organizations, and how it affects the efforts to provide reasonable assurance to the board of directors, management and other stakeholders. Internal audit must not only understand change and innovation, but must embrace, adopt, thrive with it and promote it. This course will demonstrate where and how innovation can work in your organization’s favor, so value is protected and enhanced while risks are appropriately managed. Part one of this two-part series will explore where and how innovation can work in the planning and execution of audit assignments to enhance and protect value while risks are managed.

Key learning objectives in this seminar:
• Explore how to use innovation in the planning, fieldwork and reporting stages of an audit
• Identify ways of improving internal audit methodology
• Discover techniques to be more responsive to your clients’ needs
• Adapt effectively to an ever-changing risk and controls environment
• Understand how innovation impacts your organization
• Build stronger relationships with the board and management

Engaging case studies and class exercises will be used throughout to demonstrate key concepts and put theory into practice.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Internal Audit School (OAP301) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal auditors, compliance experts, and leaders in their internal audit departments who want to develop new audit approaches, expand their current skills, re-energize the focus of their audit activities and who want to learn tips, tools and techniques to embed innovation in their internal audit methodology.

What You Will Learn
1. The Role of Innovation in Internal Audit
2. Improving Agility
3. Embracing Innovation
4. Risk Assessments
5. Innovation and GRC
6. Audit Plan Development
7. Planning
8. Fieldwork
9. Reporting

SCHEDULE
June 15-17, 2020
New York, NY
December 7-9, 2020
Orlando, FL

Available In-House (page 8).
Tuition $2395  24 CPEs
Web: misti.com/OAM225

Innovation in Internal Audit: Part 2
Innovation from an Audit Manager’s Perspective

Seminar Focus and Features
Audit managers must understand, deploy, and sustain innovation as a key characteristic of their departments. This requires understanding the conceptual and practical aspects of creativity so it can be reflected in the planning, fieldwork, and reporting aspects of each audit and consulting engagement. Innovation must be applied more broadly internally during the entire administration of the department, and externally while supporting the organization’s risk assessment process, the development of the audit plan and while interacting with all stakeholders.
Managers and directors set the direction, pace and priorities for their departments and innovation is key to:
• Becoming agile
• Enabling change effectively both inside and outside their units
• Identifying better sources and uses of evidence
• Hiring and developing innovative auditors
• Moving from a rigid mindset to one where creativity, adaptability and resourcefulness prevail

It is not enough to desire a new image for internal audit, we must find innovative ways to use our limited resources to re-brand ourselves, broaden our role, and become more effective and efficient. Part two of this two-part series of courses will look at the importance of innovation from an audit management perspective, focusing on areas such as change management, the Three Lines of Defense Model and examples of initiatives that can be implemented to demonstrate innovation in the internal audit function.

Prerequisite: Fundamentals of Internal Audit (OAG101), IT Audit School (ITG121), Innovation in Internal Audit: Part 1 (OAM225) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal auditors, compliance experts, and leaders in their internal audit departments who want to develop new audit approaches, expand their current skills, re-energize the focus of their audit activities and who want to learn tips, tools and techniques to embed innovation in their internal audit methodology.

What You Will Learn
1. Improving Agility
2. Change Enablement
3. Evidence
4. Expanding our Role
5. Management and Leadership in the Internal Audit Department
6. Innovation in the Management of the Internal Audit Function
7. Achieving a Higher Level of Thinking
8. The Three Lines of Defense
9. Best Practices

SCHEDULE
June 18-19, 2020
New York, NY
December 10-11, 2020
Orlando, FL

Available In-House (page 8).
Tuition $1995  16 CPEs
Web: misti.com/OAM226
Auditing the Manufacturing Process

Performing Operational Audits That Add Value in Manufacturing Environments

**Seminar Focus and Features**
In this intensive, three-day seminar you will explore the critical audit areas of the core manufacturing processes, targeting such risk-intensive activities as materials control, labor-hour capture, bills of material, routing, inventory valuation and variance analysis. You will learn how to identify key manufacturing data to help you objectively perform a risk assessment of all phases of the shop floor. You will discover how to identify the key aspects of every audit engagement by focusing on the most critical business factors, which in turn will maximize audit value in all areas of the conversion cycle.

Without understanding the daily activities taking place on the shop floor, it is virtually impossible to perform a comprehensive audit. Attendees will enhance their knowledge of the shop floor and learn the language spoken to become part of the conversation.

**Prerequisite:** Fundamentals of Internal Auditing (OAG101) or equivalent experience  
**Advance Preparation:** None  
**Field:** Auditing  
**Delivery Method:** Group-Live  
**Who Should Attend**
Any internal or IT auditor working in, or auditing a manufacturing company. Specifically those tasked with auditing materials control, time and labor, billing and inventory management.

**What You Will Learn**
1. Potential Audit Review Areas in the Conversion Cycle  
2. Maximizing Audit Returns: Proven Tools and Methodologies  
3. Auditing Production Planning and Control  
4. Auditing Materials Management and Control  
5. Auditing Labor and Overhead Application  
6. Auditing Inventory Valuation/Control and Product Costing  
7. Auditing Order Fulfillment, Shipping and Warehousing  
8. Auditing Fixed Assets/Equipment and Technological Change  
9. Auditing Regulatory Issues of Significance  
10. Auditing R&D  
11. Case Study

**SCHEDULE**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 12-14, 2019</td>
<td>New York, NY</td>
<td>VTR</td>
</tr>
<tr>
<td>July 13-15, 2020</td>
<td>Chicago, IL</td>
<td></td>
</tr>
<tr>
<td>December 14-16, 2020</td>
<td>New York, NY</td>
<td>VTR</td>
</tr>
</tbody>
</table>

Available In-House (page 8).  

Tuition $2395  
24 CPEs

Web: misti.com/OAP231

“Awesome course. The instructor organized the course well and kept it incredibly engaging and useful. Loved his real-life stories and examples to really drive a few points home.”

Senior Auditor  
Esterline Technologies

Auditing Supply Chain Management

Tools and Techniques to Audit Your Organization’s Supply Chain

**Seminar Focus and Features**
In this seminar you will learn about the units within organizations that are linked upstream and downstream to provide the products, services, information and finances from the source to end-user customers. You will also learn about the management of this chain, the planning and management of all activities involved in sourcing, procurement, conversion and logistics management, in addition to the coordination and collaboration that must exist between suppliers, intermediaries, third-party providers and customers. By focusing on business objectives, risks and leading practices that define essential control activities, internal auditors will acquire the skills to confidently audit their supply chain activities.

**Prerequisite:** Fundamentals of Internal Auditing (OAG101) or Auditing the Manufacturing Process (OAP231) or equivalent experience  
**Advance Preparation:** None  
**Learning Level:** Intermediate  
**Field:** Auditing  
**Delivery Method:** Group-Live  
**Who Should Attend**
Any internal or IT auditor auditing a part of their organization’s supply chain, including demand management, warehousing and inventory management, distribution and customer service.

**What You Will Learn**
1. Defining the Key Elements of Supply Chain Management and Strategies  
2. Key Problem Areas, Essential Documentation and Audit Testing  
3. Flexible and Agile Manufacturing  
4. Distribution Strategies  
5. Information Technology and Management  
6. Cash Flow Implications  
7. Globalization and Its Compliance, Operational and Strategic Implications  
8. Forecasting  
9. Customer Relationship and Service Management  
10. Demand Management and Order Fulfillment  
11. Supplier Relationship Management (SRM)  
12. Product Development and Commercialization  
13. Warehousing and Inventory Management  
14. Returns Management  
15. Value Stream Mapping and Analysis: Lean Production and Processes to Eliminate Waste

**SCHEDULE**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 16-18, 2019</td>
<td>Chicago, IL</td>
<td>VTR</td>
</tr>
<tr>
<td>May 11-13, 2020</td>
<td>Boston, MA</td>
<td></td>
</tr>
<tr>
<td>July 7-9, 2020</td>
<td>Chicago, IL</td>
<td></td>
</tr>
</tbody>
</table>

Available In-House (page 8).  

Tuition $2395  
24 CPEs

Web: misti.com/OAP234

“The training was magnificent, looking forward to future trainings taught by Dr. Hernan Murdock. The sharing of your real life experiences were on point and certainly a highlight of the training.”

Sr. Director Internal Audit  
Mueller Water Products
Mitigating Overpayment Risk and Fraud Risk in Construction Auditing

Controls to Prevent Overpayment and Enhance Fraud Detection in Construction Projects

Seminar Focus and Features
Continuing from the Fundamentals in Construction Auditing course, this program considers the risks at the conclusion of a construction project and provides essential guidance on how to avoid overpaying on the contract. Although, many organizations will be satisfied if a project comes in on budget, that does not mean that the project has been good value or that overpayments have not been made. This course will help you to verify costs charged to a construction project are appropriate and accurate.

The course will emphasize the importance of establishing a fraud hotline specifically for your construction projects to capture feedback from contractors and sub-contractors; as well as discussing techniques to investigate allegations or wrongdoing.

Prerequisite: Fundamentals in Construction Auditing (OAG130), Fundamentals of Internal Auditing (OAG101) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal auditors, C-Suite officers, project managers, risk management personnel

What You Will Learn
1. Project Closeout: Final Cost Reconciliations
   - grading the success of the project
   - evaluating the contractors and vendors
   - discuss the process of reconciling project costs and shared savings
   - construction project official file (procurement files through closeout)
2. Common Cost Overruns and Construction Cost Recoveries
   - discuss examples where controls failed and how to prevent them within your organization
   - hourly allowances and labor burden practical advice
   - contingencies, allowances, deposits, rebates: how to handle and common pitfalls
   - data analytics procedures that have yielded successful results
   - what contractual terms provide the right to audit
   - what management monitoring tools indicate overpayments
3. Whistleblowing and Fraud
   - discuss ways to prevent and minimize construction fraud
   - fraud hotline and fraud reporting
   - how to respond and investigate

Bank Internal Audit School
Understanding Banking, the Associated Risks and How to Control Them

Seminar Focus and Features
This four-day seminar is designed to provide internal auditors with the key skills that they require prior to commencing internal auditing assignments within financial service institutions. Looking at the various different components of the banking industry, the course considers the internal audit approaches that would be appropriate and assists delegates to design suitable internal audit programs for such assignments. This course is based on the application of the risk based approach and the key risks of each area will be considered throughout. Real-life examples will be used to illustrate the significance of the issues considered.

By attending this course, participants will obtain a general appreciation of the application of the risk based approach and the internal audit approaches that are suitable. Specifically they will consider the auditing approaches within:
- retail banking
- corporate banking
- private banking
- financial instruments

Prerequisite: Fundamentals of Internal Auditing (OAG101) or some knowledge of basic audit techniques and familiarity with the financial markets

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal, external, and credit auditors; audit directors and managers; CAEs; risk managers

What You Will Learn
1. How to Audit a Bank
2. Deposits and Deposit Taking
3. Funds Transmission and Clearing Services
4. Personal Lending
5. Corporate Lending
6. Security and Provisioning
7. Trade Finance and Finance of Trade
8. Branch Banking
9. Private Banking
10. Investment Banking
11. Dealing and the Dealing Room
12. Foreign Exchange
13. Forward Contracts
14. Futures and the Futures Market
15. Options and the Options Market
16. Swaps and the Swaps Market

Available In-House (page 8).

Tuition $1995  16 CPEs
Web: misti.com/OAG131
Understanding and Auditing Investments and Derivatives
Evaluating Products, Strategies and Processes

Seminar Focus and Features
In the period immediately following the financial crisis, many investments products and derivative contracts perceived as being responsible for much of the pain experienced during the downturn fell out of favor almost universally. However, many of these one-corpulm instruments and trading strategies are being revived in the post-crisis period, and financial engineering is once again producing alternative structures and positions with new risk/return profiles. Internal audit, compliance and risk management are being challenged to keep up with these developments to ensure that the proper investment and hedging processes and controls are in place to prevent another financial debacle.

This three-day seminar will provide the necessary insights to effectively evaluate the instruments, contracts and trading strategies employed by financial professionals as well as the front, middle and back office processes necessary to execute optimal investment and hedging positions. A broad variety of fixed income, equity, and alternative investments will be described, and examples of common trading and hedging strategies will be deconstructed. The regulatory and accounting implications of complex securities and hedge effectiveness testing will be presented to explain the impact that these factors have on implementing trades.

Industry-specific case studies related to both investments and derivatives will be evaluated to illustrate the potential for risk at both the institutional and systemic level. Throughout the course, specific audit approaches and test steps will be presented to ensure that delegates are developing stronger tools to evaluate the controls and processes necessary to effectively utilize a wide variety of investment instruments and derivative contracts.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Bank Internal Audit School (OAP385) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal, external and investment auditors; risk managers; middle office managers; accountants; investment compliance officers; financial institution regulators; bank examiners

What You Will Learn
1. Investment Products and Instruments
2. Derivatives for Risk Management
3. Forward-Oriented/Option-Oriented Derivative Contracts
4. Swap Contracts
5. Central Clearing Requirements
6. Controlling Investment and Derivative Risks
7. Accounting for Derivatives

Auditing Asset Management
A Practical Training Program for Learning Key Risks and Management Techniques

Seminar Focus and Features
The objectives of this course are to enable attendees to appreciate the primary issues that arise in practice when undertaking the internal audit of asset management, to ensure that the internal auditors focus on the areas of greatest risk and that they develop practical solutions to the challenges that they face. Using a series of practical case studies, attendees will develop key approaches that can be applied directly to their institutions.

This three-day training course is designed to provide course participants with an understanding of the key internal audit issues that exist within asset management. The program will concentrate on the main asset types: equity (listed and unlisted), fixed income and property, whilst referring to other available asset types. By the end of the course attendees will have built a series of audit programs that enable them to audit an asset management operation and will have an increased awareness of the primary issues and controls applied in practice. This course combines classroom lecturing and practical workshop-style learning. Case studies, exercises and role playing will be used where appropriate.

Prerequisite: None
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
This course is specifically designed for employees who are required to conduct internal audit assignments within asset management.

What You Will Learn
1. The General Asset Management Control Environment
2. Acquiring a Client
3. Quoted Equity Investment
4. Quoted Fixed Income Investment
5. The Risk Management of Alternative Investments
6. Money Market Funds
7. The Risks in Asset Allocation and Portfolio Management
8. The Risks in Outsourcing and the Selection and Management of Third Parties
9. Other Matters

SCHEDULE
June 22-24, 2020
New York, NY
October 26-28, 2020
Chicago, IL

Available In-House (page 8).
Tuition $2695 24 CPEs
Web: misti.com/OAP380
### Business Process Auditing

**A Unique Methodology for Focusing Audits on the Organization’s Core Business Functions**

**Seminar Focus and Features**

In this three-day seminar you will learn how to use Process Flow Auditing (PFA) to analyze and break down a business into its core processes and to identify high-payback areas. You will focus on operational auditing and its interaction with IT auditing to arrive at an integrated approach to audits that will help control costs, minimize risks and exposures and maximize your understanding of the business. You will explore the critical role of data in process reviews and analyses, determining how to apply business-oriented risk assessment techniques to key processes. You will also learn alternative audit tools and methodologies you can use to make your engagements highly effective and efficient, boost productivity and maximize payback.

**Prerequisite:** Fundamentals of Internal Auditing (OAG101) or equivalent experience

**Advance Preparation:** None

**Learning Level:** Intermediate

**Field:** Auditing

**Delivery Method:** Group-Live

**Who Should Attend**

Internal and IT audit staff, seniors and managers responsible for documenting internal audit walkthroughs and better understanding the flow of data, people, process and technology in a business process.

**What You Will Learn**

1. **PFA: Primary Function**
2. **Understanding the Business**
3. **Tools, Techniques and Approaches for Maximizing Efficiency**
4. **Risk-Intense/Value-Added Processes**
5. **Applying PFA to Operational Areas**
   - key operational areas and how they link to primary financial processes
   - correlating costs to risk assessment
   - key performance indicators
   - operational risks in the context of your business
   - linking operations to the corporate strategic mission
6. **Applying PFA to Key Financial Areas**
7. **Applying PFA to IS/IT**
   - identifying the organization’s core systems
   - five critical risk/control zones
   - understanding data flow
   - relating systems to the process flow review
8. **PFA Case Study**
9. **Internal Audit’s Role and Identity**

**SCHEDULE**

<table>
<thead>
<tr>
<th>Location</th>
<th>Dates</th>
<th>City</th>
<th>24 CPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 7-9, 2019</td>
<td>New York, NY</td>
<td>New York, NY</td>
<td>VTR</td>
</tr>
<tr>
<td>April 6-8, 2020</td>
<td>Washington, DC</td>
<td>Washington, DC</td>
<td>VTR</td>
</tr>
<tr>
<td>October 5-7, 2020</td>
<td>New York, NY</td>
<td>New York, NY</td>
<td>VTR</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Tuition $2395  
Web: misti.com/OAP311

### Building a Risk Model for Managing Functions Utilizing Business Intelligence

**Managing the Risks of Critical Support Functions Using Data Analytics**

**Seminar Focus and Features**

A tremendous amount of cost is incurred in those areas that are necessary to operate but are not self-supporting from a cash perspective. To manage the organization effectively on a holistic basis, it is necessary to not only effectively manage the costs of developing and delivering your products and services but also the significant cash consumers of central support, HR & technology services to name two.

In this course you will learn how to efficiently and effectively perform powerful risk assessments of every key area of central support utilizing data analytics. Employing data analytics is the only way to accurately assess every aspect of risk that can be present in these areas. This will range from the effectiveness of controls from a design and operation standpoint to the performance of the key functionalities of each of these areas. You will learn how to identify root causes of risks that are present and develop proven business cases for why management must act to correct these deficiencies. In addition, you will discover how to implement a continual risk assessment methodology for these areas.

**Prerequisite:** Risk School (OAR201) or equivalent experience

**Advance Preparation:** None

**Learning Level:** Intermediate

**Field:** Auditing

**Delivery Method:** Group-Live

**Who Should Attend**

Internal auditors, audit directors, risk management personnel, Chief Risk Officers, data analysts

**What You Will Learn**

1. **Using Data Analytics to Effectively Risk Assess Finance & Financial Reporting**
2. **Using Data Analytics to Effectively Risk Assess Legal**
3. **Using Data Analytics to Effectively Risk Assess Human Resources**
4. **Using Data Analytics to Effectively Risk Assess Marketing & Sales**
5. **Using Data Analytics to Effectively Risk Assess Technology Services**
6. **Using Data Analytics to Effectively Risk Assess ERM**
7. **Using Data Analytics to Effectively Risk Assess Outsourcing & Third-Party Contracting**
8. **Using Data Analytics to Effectively Risk Assess Purchasing**

**SCHEDULE**

<table>
<thead>
<tr>
<th>Location</th>
<th>Dates</th>
<th>City</th>
<th>32 CPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2-5, 2019</td>
<td>San Francisco, CA</td>
<td>San Francisco, CA</td>
<td></td>
</tr>
<tr>
<td>May 4-7, 2020</td>
<td>New York, NY</td>
<td>New York, NY</td>
<td>VTR</td>
</tr>
<tr>
<td>September 21-24, 2020</td>
<td>Chicago, IL</td>
<td>Chicago, IL</td>
<td>VTR</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Tuition $2695  
Web: misti.com/OAR255

TO REGISTER  CALL 508 • 879 • 7999 EXT. 501  WWW.MISTI.COM
Advanced Risk-Based Internal Audit for Banks
Implementing Practical Approaches and Techniques within Complex Banking Audit Areas

Seminar Focus and Features
This course looks at the areas where bank internal auditors face the greatest challenge. Auditing governance is always a difficult area where new approaches need to be considered to enable necessary change to be made. Scenario modeling and stress testing include a lot of judgment and provide internal auditors with a unique set of issues to deal with. Liquidity risk management has a range of new regulatory requirements and expectations that need to be addressed by internal auditors. This course takes a risk-based approach to all of these issues, including developing appropriate audit programs, and will assist internal auditors in considering how to meet regulatory and audit committee expectations.

Prerequisite: Bank Internal Audit School (OAP385) or an understanding of bank operations and products
Advance Preparation: None
Learning Level: Advanced
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal auditors, senior audit staff and audit managers who lead audits or are responsible for supervising audit staff; Audit Committee members; regulators; risk managers

What You Will Learn
1. Auditing Corporate Governance
2. Risk Appetite
3. Risk-Based Audit Planning
4. Auditing Strategy
5. Auditing Enterprise Risk Management
6. Auditing Models
7. Auditing Market Risk Management
8. Liquidity Risk
9. Stress Testing/Scenario Analysis

SCHEDULE
October 28-31, 2019
Chicago, IL
May 18-21, 2020
Miami, FL
December 7-10, 2020
New York, NY

Available In-House (page 8).
Tuition $3095  32 CPEs
Web: misti.com/OAP390

Risk Assessing Bank Operations Using Data Analytics
Building Intelligent Audit Capabilities into the Organization's Profit Drivers

Seminar Focus and Features
The one true fact about any organization is that it is the operations that determine your success or failure as an entity. Many times, not enough attention is devoted by auditors and risk personnel to the enormous number of risks that exist in operations. In this course you will become very familiar with those areas of risk that may not be properly overseen, while developing a 21st century approach to risk assessing these areas using data analytics.

The OCC has defined nine categories of risk for bank supervision purposes. Even though these are specifically defined for federally chartered institutions, these risk categories should be standard operating procedure for all financial institutions. The risk categories defined are: Credit, Interest Rate, Liquidity, Price, Foreign Exchange, Transaction, Compliance, Strategic and Reputation. As with any risk categorization scheme, the categories are not mutually exclusive; any product or service may expose the bank to multiple risks which are fluid and cannot be pigeonholed conveniently. During this seminar we will relate these categories to the operational areas of your financial institution.

In this course we will explore a number of risks in each of these categories that are the key issues of the day and the ongoing issues of tomorrow. You will leave this session with a sound basis for analyzing risk in your financial institution with the data analytics necessary to build a continual/continuous risk oversight system that will be beyond world class.

Prerequisite: Risk School (OAR201) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal auditors, audit directors, risk management personnel, chief risk officers, data analysts

What You Will Learn
1. Mapping a Financial Institution Operationally
2. Risk Assessing Credit Risk Using Data Analytics
3. Risk Assessing Interest Rate Risk Using Data Analytics
4. Risk Assessing Liquidity Risk Using Data Analytics
5. Risk Assessing Credit Risk Using Data Analytics
6. Risk Assessing Price Risk Using Data Analytics
7. Risk Assessing Transaction Risk Using Data Analytics
8. Risk Assessing Compliance Risk Using Data Analytics
9. Risk Assessing Strategic Risk Using Data Analytics

SCHEDULE
November 18-21, 2019
Chicago, IL
March 23-26, 2020
New York, NY
August 3-6, 2020
Chicago, IL

Available In-House (page 8).
Tuition $2695  32 CPEs
Web: misti.com/OAR220
High-Impact Skills for Developing and Leading Your Audit Team
Practical Strategies for Motivating Your Audit Team to Achieve Value-Added Results

Seminar Focus and Features
In this three-day seminar you will learn audit leadership tools and techniques that will enhance your role as a leader, improve the performance of your audit team and boost its profile in the organization. You will take a hard look at the skills you currently possess and master strategies that will allow you to leverage your audit knowledge with proven tactics that will inspire and motivate your staff.

You will cover the essential practices of sound audit leadership, including modern goal-setting methods, effective coaching, establishing hiring practices that will attract the best people, leading productive team and departmental meetings, and mastering the art of persuasion. You will hone your communication skills, both oral and written, and find new ways to help your team members reach their highest potential. Throughout this interactive seminar, you will use the tools you learn and receive constructive feedback from your instructor.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Advanced Auditing for In-Charge Auditors (OAG201) or equivalent experience

Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal audit seniors, managers, senior managers and directors with 5+ years of experience. Those responsible for the completion of multiple internal audit projects.

What You Will Learn
1. From Managing to Leading: Going the Distance
   - analyzing and understanding strengths and weaknesses as an audit team leader
   - manager vs. leader
   - applying leadership concepts
   - more powerful audit engagements
   - reinforcing the team ethic
   - creating a climate for sustainable competitive achievement
   - modeling and enforcing corporate values and personal integrity
   - building a leadership style
   - inspiring action by building trusting relationships

2. Essential Leadership and Management Skills
   - modern goal-setting techniques
   - emotional intelligence
   - creating powerful team agreements
   - assessing the personality styles of your team members and how to work with them
   - optimizing team productivity, evaluating team performance and measuring bottom-line results
   - managing those resistant to new ideas or change

3. Hiring and Motivating Employees
   - coaching and building an extraordinary results-driven audit team
   - establishing inter-colleague coaching
   - compelling techniques to motivate your team
   - approaches to setting direction, instructing, and training
   - giving feedback and recognition

   - how to create a positive and energized team
   - developing the right set of skills to lead by example
   - how to get the correct information during an interview
   - a systematic approach to effectively dealing with performance issues

4. Time, Stress, and Priorities Management
   - setting time management priorities
   - how to deal with the effects of stress
   - designing pre-meeting and post-meeting accountability tracking and deliverables

5. Communication Skills, Team Building, and Conflict Management
   - the four stages of team development
   - how to delegate generously and wisely
   - honing skills for participative and focused team meetings
   - how to improve listening skills and understanding travel professionals'
   - designing pre-meeting and post-meeting accountability tracking and deliverables
   - problem solving and conflict resolution strategies

   - successfully exploiting the value of competing viewpoints
   - insisting on and achieving data-based conclusions to all your audit meetings

6. Common Management Mistakes
   - avoiding confusion, mixed messages, wasted time and frustrated followers

7. Training and Mentoring Programs
   - ensuring continuous learning is rewarded
   - incorporating measurable ROI-based training
   - turning every audit manager on your team into a coach
   - creating valuable and vibrant career plans to keep the people you want
   - appreciating and assessing your teams’ training needs

8. Leading Change
   - experimenting with strategies and methods of successful influence
   - using power and influence appropriately
   - identifying and assessing your preferred style of persuasion

9. Global Auditing
   - adapting to language barriers
   - awareness of the local cultural sensitivity
   - accounting and legal differences
   - professional proficiency
   - understanding travel requirements
   - resources

10. Summary

SCHEDULE

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Tuition</th>
<th>CPEs</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 28-30, 2019</td>
<td>New York, NY</td>
<td>$2395</td>
<td>24</td>
</tr>
<tr>
<td>March 24-26, 2020</td>
<td>San Francisco, CA</td>
<td>$2395</td>
<td>24</td>
</tr>
<tr>
<td>August 10-12, 2020</td>
<td>New York, NY</td>
<td>$2395</td>
<td>24</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Web: misti.com/OAM425
Successful Audit Data Analytics for Managers
A Blueprint for Managing an Internal Audit Data Analytics Department

Seminar Focus and Features
In this two-day seminar attendees will learn what it takes to set up and run a successful data analytics, or Computer Assisted Audit Techniques (CAATs) function within an audit or compliance team. You will learn how to establish a vision, organize a team to support that vision and make effective resource and investment decisions. We will review common hurdles and hear how the most successful organizations in the world have been able to exploit the power of data analysis to achieve visible and sustainable value.

During interactive discussions and group exercises, you will get the opportunity to provide constructive feedback on an example analytic project and learn practices that can make your program more sustainable. You will learn how to challenge your team to not only build analytics for the audit, but analytics to support your future. This seminar will give you the skills you need to run a sustainable program and push it to the next level.

Prerequisite: Fundamentals of Internal Auditing (OAG101), IT Auditing and Controls (ITG101) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Audit managers, directors, and executives; IT audit managers, and directors; QA personnel; IT directors; CIOs; consultants

What You Will Learn
1. Overview of Data Analytics
2. The Internal Audit Profession and Audit Analytics
3. Data Analytics Across the Audit Process
4. Stages of the Audit Analytics Process
5. Data Analytics for Common Business Processes
6. Technologies for Audit Data Analytics
7. Maturing the Use of Audit Data Analytics
8. Best Practices for Dealing with Implementation Challenges

What You Will Learn

“Very relevant. We have been struggling between level 2-3 for some time, and feel positive about moving forward.”

Director, Corporate Audit Services
First National Bank of Omaha

Managing the Internal Audit Department
Directing and Managing a Risk-Based Internal Audit Department

Seminar Focus and Features
New business risks, governance, globalization and the continuing demands of the audit committee and senior management for value-added services combine to make the job of an internal audit manager more and more difficult. This three-day seminar is a road map to developing or maintaining an audit department that is ready to meet the challenges of this evolving business environment. Build on the key responsibilities of the audit manager and director and explore best practices in internal auditing today. Focusing on establishing a mission statement and strategic plan for internal audit, you will cover setting attainable objectives and goals; reacting to changing risk/control relationships, marketing internal audit’s services, structuring the audit department, the annual audit planning process, co-sourcing smarter and more.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Advanced Auditing for In-Charge Auditors (OAG201) or equivalent experience
Advance Preparation: None
Learning Level: Advanced
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Internal audit seniors, managers, senior managers and directors with 5+ years of experience. Those responsible for the completion of multiple internal audit projects.

What You Will Learn
1. The Critical Role of the Audit Director/Manager
2. Developing an Effective Mission/Vision Statement
3. Developing Strategic and Risk-Based Annual Business Plans
4. Corporate Governance
5. Building Relationships: Marketing and Selling Internal Audit
6. Audit Committee Relationships
7. Attracting and Keeping the Right People with the Right Stuff
8. Co-Sourcing
9. Minimizing Departmental Administration
10. Improving the Productivity of the Audit Process
11. Incorporating Best Practices Throughout the Department
12. Internal Audit’s Role in Recent High-Profile Situations and What Went Wrong—Lessons Learned

SCHEDULE

Successful Audit Data Analytics for Managers
SCHEDULE

Managing the Internal Audit Department
SCHEDULE
Audit Directors’ & Managers’ Symposium

Working Together to Develop Innovative Ways to Address Internal Audit Challenges

Program Focus and Features
Audit directors and managers are in unique positions in their audit departments. These first-line leaders are usually responsible for both helping set and determine internal audit strategy, but also directly responsible for managing those whose work will achieve internal audit’s strategy. To lead a successful risk-based department, the internal audit executive needs to have the emotional and social agility to influence their team and stakeholders to take action, be armed with the knowledge of best practices to manage the internal audit department and to leverage leading technologies to improve internal audit’s effectiveness and efficiency.

MISTI’s Audit Directors’ and Managers’ Symposium aims to equip internal audit executives to better lead their departments. This symposium will gather like-minded internal auditors to learn from subject matter experts and to share their perspectives on managing their team, improving internal audit business processes and how to leverage new internal audit technologies to maximize the value their team provides. The program will highlight methods to manage internal audit stakeholder key relationships, identify and analyze tools used to add value to audit customers and review techniques to influence change within and outside of the internal audit department.

NOTE: MISTI is still in the process of developing the 2020 agenda. Below is a look at the 2019 agenda. Keep up to date at auditsymposium.misti.com.

Prerequisite: Advanced Auditing for In-Charge Auditors (OAG201), Managing the Internal Audit Department (OAM401) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Business Management & Organization
Delivery Method: Group-Live

Who Should Attend
Newly appointed CAEs, vice presidents, directors, managers, supervisors, or internal audit managers and directors with 8+ years of internal audit experience and other members of the internal audit management team eager to improve their internal audit practices to enable positive change in their organization.

What You Will Learn

1. Enhancing Our Strategic Mindset: Adding Value in 2019 and Beyond

2. The Top Operational and Compliance Risks We Need to Address
   - overview of key risks internal auditors and compliance professionals are dealing with
   - auditing new risks and having the resources to do so

3. The Top Technology and Cybersecurity Risks We Need to Address
   - key challenges management, IT, security, compliance and internal audit professionals are facing
   - how to keep up and provide reasonable assurance when rapidly changing technological advances are the norm
   - working effectively with other assurance providers to leverage resources

4. Innovation in Internal Audit

5. Branding the Internal Audit Department
   - key actions to make the transformation from corporate cop to trusted advisor
   - becoming a change agent without losing independence or objectivity
   - convincing management that it needs the insight we can provide on strategic initiatives
   - essential steps to becoming indispensable to the audit committee
   - how to exceed our stakeholder’s expectations in terms of speed, quality and cost
   - developing and implementing a compelling mission and vision that your staff embraces

6. How to Deploy Data Analytics Effectively and Sustainably

7. Continuing to Benefit From Your Mature Data Analytics Program
   - generating ideas to constantly improve your data analytics program
   - new and innovative enhancements organizations are embracing
   - working with management to hand over the monitoring tools developed
   - getting feedback about management needs and showing them how data analytics can help
   - applying the tools more broadly in audit and consulting engagements

8. From Small to Great: Addressing the Unique Data Analytics Needs of Small and Medium Audit Departments
   - getting started and overcoming typical roadblocks: Staff, cost, data quality and lack of management support
   - sometimes you select the tool, sometimes the tool selects you
   - create it once and use it many times: Which audits lend themselves for one-time-only analytics, short-term pilot programs and ongoing monitoring activities
   - building an escalation protocol to retain your independence
   - finding help when you need it

9. Measuring and Improving the Productivity of Internal Auditors
   - implementing primary, secondary, objective and subjective performance metrics
   - using feedback to improve productivity, engagement and auditor development
   - building individual and team performance indicators
   - key conditions and behaviors that motivate, and demotivate, your staff
   - dealing with difficult employees

10. Combined Assurance: Using Technology Effectively to Do More With Less

11. Improving Agility and Persuasion: Key Skills Internal Auditors Need to be Successful

“Great way to reset, step back and re-evaluate how we can improve. Re-energized the passion I have for what I do!”

Audit Manager
Magellan

SCHEDULE
May 19-21, 2020
Hilton Head, SC

Tuition 21 CPEs
$2395 Early Price (until 3/13/20)
$2595 Regular Price
Web: auditsymposium.misti.com

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM
The Audit Executive Institute

A Master’s Program for CAEs and Audit Leaders

Program Focus and Features
Joining the best of The Audit Leadership Institute with The CAE Master’s Program, The Audit Executive Institute brings together a team of thought leaders and practitioners in internal audit to share ideas and exchange practical business solutions and best practices of highly effective audit leaders. During this four-day, two-track program, you will participate in creative problem-solving sessions, visionary planning, lively discussions, interactive presentations and networking opportunities.

Audit Leadership Track:
What does it take to successfully lead a risk-based audit department in a fast-paced, ever-changing environment? The Audit Leadership Track will look at the leadership styles that leading audit executives use, how they solve problems and how they inspire their staff. The program will cover conflict resolution, negotiation techniques and how to foster sustained organizational change. Participants will learn proven strategies to communicate better with the audit committee, the C-suite and your audit team. This track will also cover some practical and tactical skills all top audit leaders need to develop, such as assessing risk, using data analytics and keeping up with evolving technology.

CAE Master’s Track:
The CAE Master’s Track brings you and your peers together to discuss the complex and emerging issues and opportunities CAEs face. The goal is to strategically position you (and your internal audit team) as a valued contributor to the executive team, Audit Committee and Board and as a recognized business partner to your organization’s C-Suite. You will learn how others have positioned their internal audit team as the “go-to internal resource” and risk advisor/leader in the organization.

NOTE: MISTI is still in the process of developing the 2020 agenda. Below is a look at the 2019 agenda. Keep up to date at auditexecutive.misti.com.

Prerequisite: Advanced Auditing for In-Charge Auditors (OAG201) or equivalent audit management experience
Advance Preparation: None
Learning Level: Intermediate
Field: Business Management & Organization
Delivery Method: Group-Live

Who Should Attend
CAEs, vice presidents, directors, managers, supervisors and other audit executives looking to reach the upper echelon of leading an internal audit department

What You Will Learn
Audit Leadership Track:
1. Remaining Relevant Now and in the Future
2. The Art of Effective Leadership
3. Building the Right Team: Attracting and Retaining Top Talent and Optimizing Generational Differences
4. Auditing the Black Box: Possible Approaches to Auditing AI Systems
5. Recap Prior Day’s Key Content and Takeaways
6. Communicating for High Impact Results: Defusing Conflict and Managing Crucial Conversations
7. Communicating for High Impact Results: Overcoming Objections at Any Point in the Audit
8. Communicating for High Impact Results: Issuing Timely, Value-added Reports
9. What It Takes to Be The Influential and Trusted Advisor
10. Audit’s Role in Corporate Governance
11. Are You and Your Team Future-Ready?
12. Hit the Ground Running: Essential Steps to Effectively Onboard New Employees
13. Key Skills for Success
14. Going Beyond Training: How to Coach, Mentor and Develop Your Staff
15. How to Increase Staff Engagement
16. Dealing with Difficult Employees
17. Leadership vs. Inspire-ship
18. Promoting and Sustaining an Agile and Innovative Methodology and Workforce

CAE Master’s Track:
1. Improving the Identification, Analysis and Quantification of Events During Your Risk Assessments
2. Auditing What Matters Most: Developing More Effective Audit Plans and Audit Programs
3. Elevating Our Use of Data Analytics and Technology
4. How to Plan and Conduct an Audit of Corporate Culture and Ethics
5. Building Stronger Relationships and Working More Effectively with the Third Line of Defense
6. Auditing the Black Box: Possible Approaches to Auditing AI Systems
7. Tips, Tools and Techniques to Improve Our Written Communications
8. The Best Metrics to Evaluate Your Staff’s Performance
9. How to Address Technology and Change Management Risks While Constrained by Limited IT Audit Resources
10. Transforming Your Audit Department through Technology
11. Are You and Your Team Future-Ready?
12. Developing the Strategic Vision for Your Department
13. Leveraging Your Seat at the Table: Expanding the Audit Committee and C-Suite Relationships
15. Resourcing to Meet Strategic Human Capital Needs: Outsourcing, Co-sourcing, Developing Succession Talent
17. Refining the Takeaway Game Plan for Your Department
18. Promoting and Sustaining an Agile and Innovative Methodology and Workforce

SCHEDULE
August 2020
TBD
Tuition $3495* 31 CPEs
Web: auditexecutive.misti.com

(*pricing and CPEs for The Audit Executive Institute are subject to change)
IT Auditing and Controls

Auditing Technology for Business Auditors

Seminar Focus and Features
Internal or operational auditors in today’s complex organizations must understand information systems and be able to function within a technical environment. This three-day seminar outlines the concepts of information technology you need to know in order to understand the audit concerns in the IT environment. You will learn the critical business application system controls and the supporting IT general controls. You will focus on key risks and controls in such critical areas as user access to business applications, database security, networks, change management and disaster recovery. You will leave this session with a solid foundation in the basics of information technology as they apply to audit and security concerns.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal audit staff, seniors and managers responsible for performing integrated internal audits, or those who want an introduction into IT auditing.

What You Will Learn
1. Introduction to IT Risks & Controls
2. Planning IT Audits
3. Audit & Control Frameworks and Standards
4. Basics of Information Technology
5. Database Technology and Controls
6. Network Technology and Controls
7. IT Governance
8. IT General Controls
9. Business Application Controls

SCHEDULE
October 21-23, 2019
New York, NY
December 2-4, 2019
Orlando, FL
February 25-27, 2020
New York, NY
April 27-29, 2020
Boston, MA
July 13-15, 2020
Chicago, IL
August 24-26, 2020
Washington, DC
October 19-21, 2020
New York, NY
November 16-18, 2020
Orlando, FL

Available In-House (page 8).

Tuition $2395      24 CPEs
Web: misti.com/ITG101

“This was a great deep dive course that provided a good holistic approach that I found valuable to further my understanding.”
IT Audit Associate
Duke Energy

IT Audit School

An Introduction to the Essential Skills You Need to Perform IT Audits

Seminar Focus and Features
This four-day course is designed for financial, operational, business and new IT auditors to provide a solid introduction into the risks and controls necessary to audit information technologies and business application systems. We will cover the concepts of information technology as they relate to key risks in the IT environment, and explore such IT areas as operating systems, database management systems and networks. We will review IT audit concepts for auditing application systems and supporting IT general controls. Focusing on a top-down, risk-based approach to auditing application system transactions, you will learn techniques you can apply to all types of applications from batch, to on-line, to real-time systems. You will leave this intensive seminar with a solid foundation in the basics of information technology as they apply to IT risks, audit, information security and business application systems.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
IT audit staff with 0-3 years’ experience. Internal auditors with an IT background seeking an introduction to IT auditing concepts.

What You Will Learn
1. Introduction to IT Risks and Controls
2. Planning IT Audits
3. Audit and Control Frameworks and Standards
4. Basics of Information Technology
5. Database Technology and Controls
6. Network Technology and Controls
7. IT Governance
8. IT General Controls
9. Business Application Controls
10. Top-Down Risk-Based Planning
11. Executing Integrated Audits
12. Business Application Controls
13. Testing Business Application Controls
14. Documenting Business Application Controls
15. End User Computing

SCHEDULE
October 21-24, 2019
New York, NY
December 9-12, 2019
New York, NY
February 10-13, 2020
New York, NY
March 9-12, 2020
San Francisco, CA
April 6-9, 2020
Chicago, IL
May 18-21, 2020
Washington, DC
June 15-18, 2020
New York, NY
August 17-20, 2020
Orlando, FL
September 14-17, 2020
Dallas, TX
October 26-29, 2020
Atlanta, GA
November 18-21, 2020
Washington, DC
December 7-10, 2020
Orlando, FL

Available In-House (page 8).

Tuition $2695      32 CPEs
Web: misti.com/ITG121
IT Risk Management School
Fundamentals of Conducting Scenario-Based IT Risk Assessment

Seminar Focus and Features
Risk management is the primary process organizations use to determine their current capability to identify, manage and respond to risk. A properly conducted IT risk assessment gives organizations the best depiction of their ability to maintain the confidentiality, integrity and availability of their information assets. As a result, there is increased regulatory pressure from both industry and regulators for organizations to have a solid, demonstrated and thought-out process of technology risks and their potential outcomes (both positive and negative) embedded in their risk management process. This means asset identification and inventory, vulnerability and threat analysis, control inventory, risk assessment and response, risk monitoring and reporting and of course incident response, business continuity and disaster recovery.

During this event participants will be exposed to fundamental risk concepts including:
- Risk Management Strategy and Program Development
- The IT Risk Universe and it’s Key Components
- Inherent Risk Concept and Assessment Techniques
- Scenario Analysis Development Fundamentals
- Risk Response Preparation and Execution Basics

At the end of the session, attendees will have an additional perspective on the IT related risk assessment process and some of the more critical components to incorporate into any program.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Information security, IT audit and audit professionals looking to gain greater knowledge on how to perform an IT risk assessment and develop a strong IT risk management program.

What You Will Learn
1. Basic Introduction to Risk Governance and Management
2. Importance of Risk Identification and Articulating the Risk Universe
3. Assessing Inherent Risk
4. Developing Risk Scenario’s
5. Conducting Risk Assessments
6. Performing Maturity Assessments
7. Determining Risk Response
8. Risk Monitoring and Reporting
9. Tie of Corrective Controls
10. Audit Checklist

Conducting an IT Risk Assessment
Conducting a Scenario-Based IT Risk Assessment Workshop

Seminar Focus and Features
Today’s IT information security professionals need to have a working understanding on how to conduct risk assessments in a world where threats are changing by the minute. To reinforce the key concepts and best practices learned in IT Risk Management School (ITG160), this seminar is designed to walkthrough the IT risk assessment methodology by conducting multiple group exercises associated to key risk activities.

Prerequisite: Suggested to be taken after IT Risk Management School (ITG160)
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Information security, IT audit and audit professionals looking to gain greater knowledge on how to perform an IT risk assessment and develop a strong IT risk management program. Anyone who is attending, or has attended IT Risk Management School (ITG160).

What You Will Learn
1. Reiteration of Key Risk Management Terms and Concepts
2. Demonstrate “Defining a Risk Universe”
3. Examining Teams in the Risk Process
4. Reiteration of the Risk Assessment Process
5. Demonstrate “Scoping A Risk Assessment”
6. Exploring Various Risk and Control Frameworks
7. Reiteration of Key Governance Concepts
8. Demonstrate “Creating a Risk Policy Outline”
9. Demonstrate “Conducting a Mock Risk Assessment Interview”
10. Reiterating Key Considerations for Scenario Development
11. Demonstrate “Developing a Risk Scenario”
12. Reiteration of Important Risk Awareness Concepts
13. Demonstrate “Ability to Explain a Risk to Leadership”
14. Reiteration the Importance of Integration with Enterprise Risk
15. Reiteration Key Concepts of Risk Response and Monitoring

SCHEDULE
June 15-17, 2020
New York, NY
October 5-7, 2020
Dallas, TX

Available In-House (page 8).

Tuition $2395   24 CPEs
Web: misti.com/ITG160
**Introduction to IT Governance**

**How to Maximize Benefits from IT Departments**

**Seminar Focus and Features**

This course is designed for information technology and audit professionals to understand how to realize the potential and value from investments in information technology. When done well, IT governance ensures that information technology delivers value to the organization. That value is measured in terms of aligning the business to establish IT is working on things important to the business, realizing tangible benefits from the IT function, projects and services, and minimizing risks that may result from IT implementations or activities.

Governance consists of leadership, organizational structures and decision-making processes that facilitate accountability of IT activities as well as sustain and extend the organization’s strategies and priorities. Some symptoms of ineffective IT governance can include a perception that IT costs are too high, IT service levels are not consistently being met, innovation and business agility are limited by IT and that there is overlap in system resources. At the conclusion of this seminar attendees will have an in-depth understanding of how to establish and implement an Enterprise IT Governance Program.

**Prerequisite:** Foundational knowledge of information security and audit for industrial control systems

**Advance Preparation:** None

**Learning Level:** Basic

**Field:** Information Technology

**Delivery Method:** Group-Live

**Who Should Attend**

Information technology and security professionals, IT auditors, IT management, audit management

**What You Will Learn**

1. Introduction and Role of Enterprise IT Governance
2. Goals of Enterprise IT Governance
   - strategic alignment
   - benefits optimization
   - risk minimization
3. Elements of Enterprise IT Governance
   - decision making processes, frameworks and authorities
   - IT policies, principles and standards
4. Developing an IT Governance Strategy
   - legal and regulatory aspects
   - supplier governance
   - technology architecture governance
5. IT Governance Assessments
   - IT capability
   - organizational readiness for change
6. IT Governance Structures and Relationships
   - IT Steering, Project and Advisory Committees
   - RACI charts
7. IT Investment Management
8. Governance Metrics
   - balanced scorecard
   - ITIL metrics
   - SMART metrics
9. Audit Considerations for Enterprise IT Governance

**SCHEDULE**

- March 9-11, 2020
  - Chicago, IL
- June 1-3, 2020
  - Denver, CO
- November 16-18, 2020
  - New York, NY

**Available In-House (page 8).**

- Tuition $2395
- 24 CPEs
- Web: misti.com/ITG120

---

**Fundamentals of Auditing**

**Process Automation**

**Optimizing Process Capabilities Through Automation**

**Seminar Focus and Features**

Enterprises of all shapes and sizes are looking to see how automation can give them the advantage over their competition and aide in maintaining the increased pressure of regulatory compliance. In this three-day session, we will provide a high-level overview of the important changes you need to plan for as automation begins to transform IT and business processes. Attendees will learn the differences between process automation and DevOps, the importance of governance and ethics in automation, how to understand workflows and gain tips to assessing automation.

**Prerequisite:** None

**Advance Preparation:** None

**Learning Level:** Basic

**Field:** Auditing

**Delivery Method:** Group-Live

**Who Should Attend**

Auditors, information security and risk professionals wanting to gain a general understanding of process automation and how to assess BPM/RPM applications and servers.

**What You Will Learn**

1. Automation Explained
   - explore basic concepts about business process automation
   - explore basic concepts of robotic process automation
   - explore basic concepts of DevOps
   - discuss the differences between BPM/RPM and DevOps
2. Governance and Management of Automation
   - understand why automation requires effective governance
   - discuss the fundamental activities performed by Automation Governance Committees
   - explore common measurements to assess the effectiveness of process automation program initiatives
   - describe automation strategy and program
3. Ethics of Automation
   - describe automation ethics
   - assess common ethical challenges associated to automation
4. Understanding Workflows—Automation of IT and Business Processes
   - discuss where automation is being implemented into common IT and business processes
   - explain why a maturity assessment is critical before automation is considered
   - discuss key automation controls
   - discuss common automation vulnerabilities
5. Tips for Assessing Automation
   - overview of process automation self-assessment activities
   - explore testing activities when conducting a process automation audit
   - review key data requests when conducting a process automation audit
   - examine common questions to ask during process automation audits

**SCHEDULE**

- October 9-11, 2019
  - New York, NY
- February 24-26, 2020
  - Orlando, FL
- July 22-24, 2020
  - Chicago, IL

**Available In-House (page 8).**

- Tuition $2395
- 24 CPEs
- Web: misti.com/ITG170
Cybersecurity Audit School
Understanding the Auditing Methodology Regarding Cyber Engagements

Seminar Focus and Features
Armed with motive and skill, hackers and internal bad actors continue to release more sophisticated exploits taking advantage of opportunities of “weaknesses” in our environments. Tomorrow’s auditor needs to know more than just the terms and concepts regarding cybersecurity. They need to understand what controls are needed, where the controls should be positioned and how to perform substantive tests to assess the controls reasonable effectiveness related to cybersecurity.

During this seminar attendees will have the opportunity to conduct a mock cybersecurity program audit. By the end of the session attendees will be armed with the knowledge of how to perform an assessment on a company’s cybersecurity program and should become more valued members of their organization’s cyber defense team.

Prerequisite: Fundamentals of Internal Audit (OAG101), IT Audit School (ITG121) or equivalent experience
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Internal and IT auditors tasked with assessing cybersecurity related processes

What You Will Learn
1. What is Cybersecurity?
2. Cyber Trends
3. Regulatory Impact
4. Cybersecurity and Data Privacy Law and Ethics
5. Hot Topics
6. Cybersecurity Vulnerability, Threat and Risk Landscape
7. The OSI Model
8. CIS Top 20 V7.1
9. Application Protections
10. Other Protections—Drilling Down a Bit Further
12. Investigation Techniques
13. Cyber Awareness—Human Firewall
14. Fundamentals of Auditing a Cybersecurity Program

Auditing a Cybersecurity Program
Simulating a Cybersecurity Auditing Engagement

Seminar Focus and Features
The audit risk universe is expanding faster than in any time in recent memory. One particular area of explosion is cybersecurity, as exploits over the last several years have heightened so has the awareness of senior leaders and boards alike.

Auditors need to be able to assess the effectiveness of an enterprise’s cybersecurity program. They need to understand what controls are needed, where the controls should be positioned and how to perform substantive tests to assess the controls effectiveness related to cybersecurity.

During this seminar attendees will simulate an actual cybersecurity program audit, vulnerability and threat analysis and cyber risk assessments. Attendees will have the opportunity to conduct a series of exercises which are designed to establish or reinforce the attendee’s knowledge of effective control design and execution. By the end of the session attendees will be armed with knowledge of how to perform cyber assessments and become a more valued member of their organization’s “Cyber Defense Team.”

This session will also provide an audit and self-assessment checklist along with examples of various cybersecurity program artifacts.

Prerequisite: Strongly suggested to be taken with Cybersecurity Audit School (ITG250).
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Auditors and IT professionals interested in conducting cybersecurity audits, risk assessments, vulnerability and threat analysis or control self-assessments. Anyone attending, or who has attended, Cybersecurity Audit School (ITG250).

What You Will Learn
1. Vulnerability Assessment
2. Threat Analysis
3. Cybersecurity Risk Assessment
4. Cybersecurity Program
5. Conducting a Cybersecurity Audit Based on the Top 20 Controls Identified in Critical Security Controls (CIS) V6.1

"This was an excellent class. The instructor was very knowledgeable on the subject matter, and did a great job of presenting. The course materials are very well documented and will be a great resource for our audit department.

Sr. Internal IT Auditor
PVH Corp.
Auditing Agile and Scrum Development Projects
Improving Project Management Through Integrated Audits

Seminar Focus and Features
Today, application systems development is all about SPEED. Agile and Scrum are all about getting data and processing and reporting to the customer ASAP. This is further complicated by the lack of standardized methodologies, expectations and business models. Auditors, reviewers and project sponsors are further confounded by the difficulty of knowing what can be done in a definitively short amount of time, especially in an environment that discourages oversight and audit. This course is designed to remove the complication, identify what auditors and developers can do to facilitate and achieve success and provide risk-based awareness of what can go right and what can go wrong with Agile and Scrum development. Key risk-based “triggers” will be provided that heighten awareness of how to review, manage and audit these “moving targets”. This course provides this unique tool that will set you on a path of contributing without distracting.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and IT auditors auditing system development projects using agile or scrum methodology.

What You Will Learn
1. What Exactly are Agile and Scrum?
2. How to Learn about the Project in Time to Get Involved
3. Definitions of Success vs. Failure
4. The Infrastructure That Should Be in Place Before the Project Begins
5. What to Look for Before the Project Begins
6. The Project Manager
7. The Steering Committee
8. The Project Plan
9. What to Look for During the Project and the Key Triggers to Apply
11. Don’t Trust the Interfaces
12. Change Management
13. Reporting Deficiencies

"Being new in my position/company and tasked with learning about how to audit agile, this course provided me with the skills to implement at my company and to teach others. The instructor was very knowledgeable and delivered the material in a manner that was easy to learn and engaging."

Audit Project Manager
Regions Bank

SCHEDULE
November 7-8, 2019
San Diego, CA

April 30-May 1, 2020
Boston, MA

June 18-19, 2020
New York, NY

December 17-18, 2020
San Francisco, CA

Available In-House (page 8).

Tuition $1995  16 CPEs
Web: misti.com/ITG213

Auditing Oracle’s® ERP Cloud Application
Key Elements of Oracle’s ERP Cloud Applications

Seminar Focus and Features
Oracle’s latest home-grown application built on Fusion technology is Oracle’s bet for the future for enterprise applications in the cloud. Oracle has used the “best of” its various applications it has bought (E-Business Suite, PeopleSoft, JD Edwards, Siebel, etc.) and built in the design of this new cloud application. In this two-day class, we will look at the core elements of the application. We will review foundational principles such as the technical architecture, security model, role design, generic users, patching and change management, common elements, profile options, controls monitoring and reporting, audit policies, workflow issues, master data, and application controls.

NOTE: Attendees are encouraged, but not required, to bring a laptop. This course will be a combination of direct teaching and interactive activities to the extent that the attendees have access to their organization’s instance.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal auditors, IT auditors, functional and IT teams implementing or supporting Oracle’s ERP Cloud applications.

What You Will Learn
1. Architectural Overview
2. Common Elements
3. Organization Structure
4. Master Data Overview
5. Building a Proper Audit Trail
6. Application Security Configurations and Administration
8. Workflow Security and Controls
9. Risks and Controls Related to Privileged Users
10. Change Management Best Practices
11. Designing and Auditing Application Controls
12. Protecting Sensitive Data in Production and Non-Production
13. Project Risks and Implementation Audits
14. Common Audit Issues
15. Auditor Resources

SCHEDULE
December 5-6, 2019
Orlando, FL

April 9-10, 2020
Denver, CO

July 16-17, 2020
Chicago, IL

Available In-House (page 8).

Tuition $1995  16 CPEs
Web: misti.com/ASE151
Auditing and Securing Oracle® Databases

A Case Study Using the Security and Integrity Features in Oracle to Perform Control and Security Assessments

Seminar Focus and Features
In this comprehensive, four-day seminar, you will learn Oracle’s database capabilities and terminology along with the activities needed to provide security and control over Oracle software. You will uncover the risks Oracle introduces, as well as the exposures it reduces. You will explore Oracle’s approach to the client/server and web processing environments and discover the impact Oracle has on enterprise organization, security profiles and information technology standards.

Using a case study, you will start with planning an audit or review and determine what technical evidence you will need. You will then analyze real-world examples of data dictionary, view reports, parameter specifications, scripts and trace data for evidence of security and integrity problems. You will learn the steps to prepare for an interview with the Database Administrator (DBA), and to present your report with technical findings and recommendations. In addition, class exercises throughout the session will reinforce course material, and you will receive an audit and security program checklist you can put to use immediately.

Prerequisite: A working knowledge of Windows or Unix system controls
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Experienced IT auditors; quality assurance personnel; data security specialists; audit managers; database and systems administrators.

What You Will Learn
1. Oracle Environments
2. Oracle Objects
3. The Security Mechanism
4. Security Features
5. Oracle Support and Security Patches
6. Database Auditing
7. Additional Areas for Controls
8. Organizational Impact
9. Audit and Security Approaches
10. Wrap-Up

Web: misti.com/ASE351

Auditing Oracle’s® E-Business Suite
An Introduction to the Applications’ Architecture

Seminar Focus and Features
Oracle’s E-Business Suite offers a wide variety of applications which require specific audit programs. Auditors and those implementing and supporting Oracle’s E-Business Suite need actionable information about the associated risks and controls. This foundational, three-day course will take you from a basic understanding, to an intermediate understanding of application risks and controls for the most commonly implemented applications along with the elements common to all implementations. We will delve deeply into application security and other IT general controls and provide you with dozens of SQL queries frequently used in assessments.

Prerequisite: Auditing Business Application Systems (ITG103) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Internal and external auditors; audit managers; those implementing and supporting Oracle’s E-Business Suite

What You Will Learn
1. Oracle Overview
2. Common Elements and Modules
3. Organization Structure
4. Master Data Overview
5. Building a Proper Audit Trail
6. Oracle Security Basics
9. Designing and Auditing Application Controls
10. Best Practices for Protecting Sensitive Data
11. Foundation/Core Application: Risk and Controls
12. General Ledger: Risks and Controls
13. Assets: Risks and Controls
14. Cash Management: Risks and Controls
15. Procure to Pay: Risks and Controls
16. Order to Cash: Risks and Controls
17. Inventory: Risks and Controls
18. Hire to Termination: Risk and Controls

Web: misti.com/ASE355

SCHEDULE
November 4-6, 2019
New York, NY

April 6-8, 2020
San Diego, CA

July 13-15, 2020
Chicago, IL

Available In-House (page 8).
Tuition $2395
24 CPEs

SCHEDULE
October 7-10, 2019
Washington, DC

April 27-30, 2020
Burlington, MA

Available In-House (page 8).
Tuition $2695
32 CPEs

Web: misti.com/ASE351
Audit and Security of SAP® ERP

Controlling and Managing Risks in SAP ECC and S/4HANA Systems

Seminar Focus and Features
In this four-day seminar, attendees 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 both its S/4HANA system and the SAP Governance, Risk and Compliance (GRC) suite of applications, and review the auditing and monitoring changes required to move down these paths.

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: IT Auditing and Controls (ITG101), IT Audit School (ITG121) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Financial, operational, business application and IT auditors; audit directors and managers; compliance managers; SAP security and support personnel

What You Will Learn
1. SAP Audit Fundamentals
2. Basic Navigation for Auditors
3. SAP Security
4. SAP Administration and Change Control
5. SAP Modules
6. FI: Financials and CO: Controlling Risks and Controls
7. MM: Materials Management Risks and Controls
8. SD: Sales and Distribution Risks and Controls
9. Other Modules (based on class interest)
10. SAP Governance Risk and Compliance (GRC) Solutions
11. Advanced SAP Auditing Techniques
12. Implementations and Upgrades

SCHEDULE
December 17-20, 2019
Dallas, TX

April 14-17, 2020
New York, NY

June 1-4, 2020
Denver, CO

September 14-17, 2020
Philadelphia, PA

December 7-10, 2020
Atlanta, GA

Available In-House (page 8).

Tuition $3095 32 CPEs

Web: misti.com/ASE241

Advanced SAP® ERP and SAP S/4HANA Audit and Security

SAP Basis System Settings and Secure Netweaver and Fiori Configuration

Seminar Focus and Features
This three-day course will provide participants with an in-depth understanding of SAP Basis and security assessment techniques necessary for performing a deep-dive technical audit. You will learn the advanced risks and control opportunities that should be considered in a thorough audit of the SAP Basis system, including considerations when using SAP GRC.

On completion of this course, attendees will be able to develop an effective SAP technical audit plan and prioritize key steps, discuss techniques for controlling both dialog and non-dialog user security, assess the appropriateness of SAP Basis configuration settings, recommend procedures for controlling customizations, analyze SAP Basis and security-related tables and describe effective research techniques related to advanced SAP technical issues. Attendees will explore changes introduced by SAP S/4HANA, specifically related to the implications of HANA and Fiori on the SAP security model. On completion of this course, attendees will be able to develop an effective SAP technical audit plan and prioritize key steps, discuss techniques for controlling both dialog and non-dialog user security, assess the appropriateness of SAP Basis configuration settings, recommend procedures for controlling customizations, analyze SAP Basis and security-related tables and describe effective research techniques related to advanced SAP technical issues.

Participants will explore newer issues around SAP cybersecurity and see demonstrations of techniques used for hacking SAP.

Prerequisite: Audit and Security of SAP ERP (ASE241) or equivalent experience

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
IT audit and SAP security personnel, as well as people in compliance or related functions that explore technical SAP risks and controls in details.

What You Will Learn
1. Reviewing the Basics
2. Advanced SAP System Parameters
3. Advanced SAP Basis Security
4. Controlling Non-Dialog User Types
5. Netweaver Security
6. Advanced Auditing of SAP Customizations
7. Hacking SAP (aka: Hardening SAP Against Hacking)
8. Analyzing SAP Tables
9. New Issues with S/4HANA

SCHEDULE
February 24-26, 2020
San Diego, CA

July 20-22, 2020
New York, NY

Available In-House (page 8).

Tuition $2795 24 CPEs

Web: misti.com/ASE441
Securing and Auditing Virtualized Environments
Best Practices for Securing and Auditing VMware ESX and Microsoft Hyper-V

Seminar Focus and Features
In this five-day seminar you will focus on ESX and Hyper-V security. You will start with virtualization basics, hardware virtualization considerations and different versions of ESX. You will examine best practices for securing ESX servers, access to the management console, ESX logging and other configuration issues to ensure your ESX virtual server hosts are secure and stable. You will then review Hyper-V and best practices for securing a Hyper-V environment. Finally, you will tie all of these concepts together with a formulation of a suggested audit program of ESX/Hyper-V and the virtual server environment.

Case studies using a combination of live demonstrations and exercises will reinforce important virtualization concepts and associated audit points addressed in real audit projects.

Prerequisite: A working knowledge of operating system security, networking concepts and associated logical access controls; Network Security Essentials (ASG203), Intermediate IT Audit School (ITG241) or equivalent experience

Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Information security managers, analysts and administrators; IT managers, architects and developers/integrators; IT auditors; network and system administrators; security architects and engineers; application certification/quality assurance specialists; consultants; compliance officers; project managers.

What You Will Learn
1. Virtualization Basics
2. vSphere/ESX Basics
3. Hyper-V
4. Virtualization and Disaster Recovery
5. Developing an Audit Program for ESX
6. ESX Case Study

Auditing Vendor Management
Evaluating the Controls and Processes for Effective Vendor Management Audits

Seminar Focus and Features
Vendor Management has become an important topic for auditors in the last three years because significant amounts are often spent without proper oversight and management. This typically results in organizations spending more than necessary while relying on vendors whose quality and practices may be inconsistent with your expectations.

This seminar addresses the risks related to vendor screening and performance, and the best techniques to monitor them. Identifying issues is certainly important, but it is also essential to avoid engaging questionable vendors so this seminar provides techniques to prevent this problematic condition. Participants will examine the objectives, risks and controls specific to this process, and through discussions, exercises and a case study, practice what is learned.

Don’t wait until a costly issue surfaces requiring investigation and remediation. Learn how to audit this high-risk process effectively, save your company money, prevent reputation damage, and avoid the problematic conditions that poor vendor contracting can lead to.

Prerequisite: None
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Financial, operational and IT auditors, vendor managers, legal counsel, purchasing/procurement personnel

What You Will Learn
1. Governance
2. Vendor Selection
3. Contracts
4. Software Vendor Management
5. Performance Monitoring
6. Exposures
7. Hardware Vendor Management
8. Cloud Service Providers and 3rd Party Computing Vendors
9. Access Management
10. Data Protection
Audit and Control of DevOps
Risk-Based Audit and Control of the Next Generation of Systems Development

Seminar Focus and Features
Software development today cannot be “business as usual”. Customers, users and management are demanding, even expecting, faster product-to-market delivery of new technologies, services and products. To seize this initiative, business owners, developers, operations personnel, quality assurance, testers, security specialists, suppliers and marketers need to work closely in a collaborative manner to deliver software in a continuous manner that puts your business ahead of the competition. This is DevOps. It is not always easy to understand or apply. It is all about continuous development, testing, deployment, monitoring, feedback, vulnerability scanning and auditing!

Auditors need to know how to audit in the continuous process, where to find the risks, how to get to them, what to do and where to focus once you are there. This course is designed to eliminate the complicated clutter, identify what auditors and developers can do to help achieve success, and provide a risk-based approach to auditing both dynamically and knowledgeably as a contributor and not a distractor.

Prerequisite: Auditing Business Application Systems (ITG103), Intermediate IT Audit School (ITG241), Auditing Agile and Scrum Development Projects (ITG213), or equivalent experience

Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
IT auditors, information security professionals, risk managers and those assigned to form or participate in a DevOps Governance Committee who wish to gain an understanding of how to govern, manage and assess a DevOps environment.

What You Will Learn
1. What Exactly is DevOps?
2. The DevOps Lifecycle
4. Top 10 DevOps Myths—and Why They Are Wrong
5. Top 10 Problems That Cause DevOps to Fail and How to Spot Them
6. Top 10 DevOps Controls
7. Can the Cloud Be Part of the Solution?
8. How to Audit DevOps
9. DON’T Trust the Interfaces
10. Continuous Delivery—This Is Not Your Parent's Change Management!
11. Reporting Deficiencies

Intermediate IT Audit School
A Risk and Compliance Approach to Auditing the IT Environment

Seminar Focus and Features
In this practical four-day seminar, attendees will immerse themselves in a risk and compliance approach to IT auditing to protect the confidentiality, integrity and availability of information assets throughout an enterprise. We will discuss how you can use common frameworks and standards as an overall framework for planning IT audits. To help arrive at organization-specific risk and compliance IT auditing benchmarks, we will identify authoritative sources for audit program requirements associated with major US and international government and industry legislation, standards, and frameworks. We will concentrate on determining risk and compliance levels in such critical management and technical areas as IT governance, information security, operating systems, database management systems, network infrastructure security, application software development, change management and business continuity planning.

Prerequisite: IT Auditing and Controls (ITG101), IT Audit School (ITG121) or equivalent experience. Familiarity with standard IT technologies, tools and controls is assumed.

Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
IT auditors with 3-7 years experience. Those tasked with planning technical IT audits, those looking to leverage common compliance frameworks.

What You Will Learn
1. Risk Assessment and Audit Planning
2. Compliance Management: Regulations, Standards and Frameworks
3. IT Governance
4. User Access Controls
5. Encryption Demystified
6. Network Perimeter Security
7. Operating System Software
8. Database Management Systems (DBMS)
10. Business Continuity and Disaster Recovery Planning
11. Auditing Outsourced IT Operations
12. Executing IT Audits

SCHEDULE
October 9-11, 2019
Chicago, IL
June 15-17, 2020
New York, NY
December 1-3, 2020
San Diego, CA
Available In-House (page 8).
Tuition $2395 24 CPEs
Web: misti.com/ITG214

SCHEDULE
September 30-October 3, 2019
Atlanta, GA
November 4-7, 2019
Dallas, TX
December 9-12, 2019
Orlando, FL
Available In-House (page 8).
Tuition $2695 32 CPEs
Web: misti.com/ITG241

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM
Advanced IT Audit School

Comprehensive Deep-Dive of IT Audit and Information Security Assessments

Seminar Focus and Features
In this information-packed four-day seminar, we will cover, in depth, key building blocks of IT audit and security, including identity and access management, web-based e-commerce application threats and vulnerabilities, as well as standards associated with privacy issues and intellectual property concerns. We will place special emphasis on discovering best practices and standards for auditing web (HTTP) servers and application servers and walk away with tools, techniques and checklists for discovering and testing web and application server security. We will also cover auditing database management systems within the context of robust but practical enterprise architecture and governance models and go over web services and service-oriented architectures including SOAP, ReST, SOA and ESB. Together, we will also review safeguard concepts and best practices for secure mobile and wireless applications.

Prerequisite: Intermediate IT Audit School (ITG241), or Network Security Essentials (ASG203), or equivalent experience. Familiarity with basic IT controls terminology and concepts is assumed.

Advance Preparation: None
Learning Level: Advanced
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
IT, internal or external auditors, IT audit managers, information security managers and analysts with 5+ years of experience, or those tasked with auditing web servers, application services, database management systems and enterprise architecture

What You Will Learn
1. Identity and Access Control Management (I&ACM) Architecture
   • information technology security standards
   • information security goals
   • distributed computing control and security risks
   • essential I&AM Policies and Standards GTAG, COSO, ISO 27002
   • information classification
   • risk analysis
   • data breach statistics
   • data security policies
   • secure application design criteria
   • security services—access control, authentication, authorization
   • access control models and architectures
   • security audit log management in multi-tiered applications
   • TCP/IP network risk analysis
   • client/server and middleware security for multi-tiered applications
   • enterprise directory services, LDAP
2. Web Application Architectures
   • protecting the web server, perimeter security, demilitarized zones
   • HTTP protocol and state management
   • SSO (single sign), pros and cons
   • web application markup languages
   • fundamentals of cryptography, ISO 27002 – 10, TLS, PKI, digital signatures
   • web application threats and vulnerabilities
   • cloud computing and security
   • web application attacks and security strategies
3. Auditing Web (HTTP) Servers
   • summary of baselines for secure server security
   • physical threats, vulnerabilities, risks, and countermeasures
   • information storage media protection, sanitization and disposal
   • locating control points in complex, multi-tiered applications
   • security awareness
   • emergency procedures
   • human resources controls: hiring practices, badges, terminations and transfers
   • goals for information security safeguards in applications
   • ISO 27002 -13 communications security
   • web server configuration: operational and security requirements
   • web server access control security features: Apache, Microsoft IIS
   • perils and protections for remote web application development
   • application firewalls and intrusion prevention systems
4. Secure Application Design, Testing and Audit
   • server-side web page programming security
   • mobile code security
   • common security vulnerabilities and attacks on web application software
   • attacks on web servers: cross-site scripting, SQL injection, buffer overflow
   • input validation and editing, SQL injection
   • software change controls and configuration management
   • web application vulnerability and testing tools
   • tools, techniques and checklists
5. Auditing Application (Middleware) Servers
   • roles, architecture and security control points for XML/object-oriented development
   • environments and associated application servers
   • defining key sources of application server security: declarative vs. programmatic controls, database and Enterprise Information System (EIS) connectors
6. Auditing Database Management Systems
   • data access control, authorization and audit
   • ISO 27002 -12 operations security
   • relational database management systems (DBMS)
   • Structured Query Language (SQL)
   • security risks associated DBMS systems
   • audit and security features for major DBMS products
   • database security safeguards, access controls, roles
   • database triggers, DDL triggers, DML triggers
   • database encryption
   • DBMS audit logging
   • database connectors
7. Web Services and Service-Oriented Architectures (SOA)
   • Simple Object Access Protocol (SOAP) web services definition and architecture
   • Service Oriented Architectures (SOA)
   • SOA Enterprise Service Bus (ESB)
   • Representational State Transfer (REST) web services
   • web services audit and security tools, and techniques
8. Mobile Application Security and Audit
   • key control points in remote access and mobile applications
   • how mobile application differ from internal server-based applications
   • checklist for secure mobile and wireless application best practices
9. Laws and Standards Affecting IT Audit
   • organizational liabilities
   • ethics affecting information security
   • international laws, directives, and regulations
   • EU Data Protection Regulation
   • world-wide impact of GDPR
   • investigations and evidence of computer crimes
   • incident response
   • intellectual property, copyright laws, and software piracy
   • prominent US and international laws

SCHEDULE

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 21-24</td>
<td>New York, NY</td>
</tr>
<tr>
<td>February 3-6</td>
<td>San Diego, CA</td>
</tr>
<tr>
<td>May 18-21</td>
<td>Washington, DC</td>
</tr>
<tr>
<td>August 17-20</td>
<td>Boston, MA</td>
</tr>
<tr>
<td>October 19-22</td>
<td>New York, NY</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Tuition $2695
32 CPEs

Web: misti.com/ITG341

VIRTUAL CLASSROOM AVAILABLE
BOLD DATES INDICATE TRAINING WEEKS
Securing and Auditing Your Network Infrastructure: Network Services, Devices and Perimeter Security

Assessing Your Network Security—Inside and Out

Seminar Focus and Features
In this down-to-earth, hands-on seminar, we will clearly identify and demonstrate practical methods to document and audit the critical safeguards in numerous forms of common wired and wireless network technologies and infrastructures used in most modern organizations.

To equip you with the necessary knowledge and audit tool awareness, we guide participants through a relevant series of practical hands-on exercises to test network security controls from the “outside” in as well as the “inside out”. We will provide the opportunity to use a wide array of built-in/bundled, open source and low-cost commercial software tools to ensure widespread applicability and affordability when the participant goes back to the office to apply the lessons learned in real life.

All exercises are documented, highlighting the security and IT audit objectives and evidence gathering and analysis procedures and can be easily incorporated into work programs. Participants will also receive valuable checklists/work programs along with references for supportive information and audit tools.

Prerequisite: Intermediate IT Audit School (ITG241), Network Security Essentials (ASG203), CISSP, CISA or equivalent knowledge of or experience in the area of networking fundamentals

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal and external IT auditors performing general controls and application audits; IT security and compliance professionals who perform technical software security audits and risk assessments.

What You Will Learn

1. Network Security and Audit Essentials
2. Protecting Physical/Media Network Access
3. Securing and Auditing Wireless Networks
4. Managing Network Application Services Cybersecurity Risks
5. Securing and Auditing Enterprise Network Address Management and Directory Services
6. Network Appliances: Functionality, Management, Security and Audit
7. Securing and Auditing DMZ Networks

SCHEDULE

<table>
<thead>
<tr>
<th>Session</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>October 7-11, 2019</td>
<td>San Diego, CA</td>
</tr>
<tr>
<td>2</td>
<td>May 18-22, 2020</td>
<td>Washington, DC</td>
</tr>
<tr>
<td>3</td>
<td>July 13-17, 2020</td>
<td>Chicago, IL</td>
</tr>
<tr>
<td>4</td>
<td>November 16-20, 2020</td>
<td>New York, NY</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Tuition $3295 40 CPEs

Web: misti.com/ASG231

Securing and Auditing Your Application Software Infrastructure: Operating Systems, Web Servers and Databases

Ensuring a Strong System Software Foundation for Distributed Business Applications

Seminar Focus and Features
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 (ITG241) or equivalent knowledge in the area of logical access controls

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal and external IT auditors performing general controls and application audits; IT security and compliance professionals needing to perform technical software security audits and risk assessments.

What You Will Learn

1. Software Infrastructure Essentials
2. Securing and Auditing Operating Systems and Other System Software
3. Securing and Auditing Windows Server/Active Directory
4. Securing and Auditing Unix/Linux Systems
5. Securing and Auditing Database Management Systems
6. Securing and Auditing Your Web Server

SCHEDULE

<table>
<thead>
<tr>
<th>Session</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>January 27-31, 2020</td>
<td>San Diego, CA</td>
</tr>
<tr>
<td>2</td>
<td>June 15-19, 2020</td>
<td>Charlotte, NC</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Tuition $3295 40 CPEs

Web: misti.com/ASG232
Introduction to Information Security
Establishing a General Understanding of Information Security

Seminar Focus and Features

This course is designed to introduce information security best practices to the non-information security professional, beginning information security professional or non-technical business professional. It provides a broad overview of information security topics including compliance, governance, network design, application security, security processes and development of an information security program. Information security frameworks are introduced to provide the attendee with the basics of information security controls. Case studies and attack methods are presented to illustrate the importance of the various elements of information security programs.

During this three-day seminar, attendees will learn how to respond to the increased emphasis on information security by gaining an understanding of how to organize and oversee a risk-based enterprise information security program. We will drill down to the critical building blocks of information security, explore the respective roles and responsibilities of the key players, discover industry best practice, legislation, and professional standards and leave the course with ideas and strategies for improving the security posture of their organization.

Prerequisite: None
Advance Preparation: None
Learning Level: Basic
Field: Information Technology
Delivery Method: Group-Live

Who Should Attend
Professionals across all businesses and sectors with 0-4 years of experience who need to know more about information security; financial, operational, business application internal and external auditors and risk managers.

What You Will Learn

1. The Case for an Information Security Program
- cyber-liability insurance
2. Security, Privacy, and Compliance
- assessments vs. audits
3. Information Security Frameworks
- NIST
- PCI
- CIS
- HIPAA
- COBIT
4. Legal and Regulatory Considerations for Information Security
- governance
5. Fundamental Information Security Concepts
- security program goals
- defense in depth
- AAA—authentication, authorization, accountability
- architectural principles
6. Tenets of Information Security
- confidentiality, integrity and availability
7. Security Program Development
- risk based approach to security
- governance
- controls
- policies & procedures
8. Network Design and Engineering
- secure network design principles
- identity and access management
- asset management
- change management
- configuration management
- data protection and management
10. Threat and Vulnerability Management
11. Cryptography Basics
12. Secure Software Development
- SDLC
- Agile
- OWASP
- software development best practices
13. Incident Response
- incident and problem management
- incident detection
- IR plans
14. Business Continuity and Disaster Recovery
- business impact assessments
- developing BC/DR plans
15. Managing and Monitoring Security of Third Parties
- MSSPs
- business partners
- cloud
16. Developing Security Metrics
17. Common Attack Methods
18. Digital Forensics

SCHEDULE

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 27-29, 2020</td>
<td>Boston, MA</td>
</tr>
<tr>
<td>July 13-15, 2020</td>
<td>Chicago, IL</td>
</tr>
<tr>
<td>October 19-21, 2020</td>
<td>New York, NY</td>
</tr>
</tbody>
</table>

Available In-House (page 8).
Tuition $2395 24 CPEs
Web: misti.com/ISG101
Network Security Essentials
A Comprehensive Introduction to Network Control Points and Associated Safeguards

Seminar Focus and Features
In this three-day seminar you will review the basic operating characteristics and risks associated with LANs, WANs, client/server and other forms of networking and distributed computing architectures. You will survey best practices for securing and auditing network applications, interconnection devices and remote access and perimeter security services. You will also map and organize the use of built-in and add-on tools to security policy and audit requirements to determine the essential topics that must be addressed in compliance and risk management, security administration standards and procedures and audit programs. You will receive security and audit checklists at the end of each control-related section.

Prerequisite: IT Auditing and Controls (ITG101), IT Audit School (ITG121) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Information security professionals or IT auditors working with networks.

What You Will Learn

1. Defining the Distributed Information Technology Environment
   - network terminology
   - computing models: centralized and distributed
   - shared data networks
   - distributed computing: client/server, peer-to-peer, middleware
   - defining the scope of network security and audit programs
   - locating network security control points

   - understanding internet technical documents
   - network protocol rule; protocol stacks: frameworks for networking
   - open systems interconnection (OSI) reference model
   - transmission control protocol/internet protocol (TCP/IP)
   - encapsulation, information formats, addressing layers
   - OSI layer risk analysis
   - IEEE 802.x wired and wireless standards and technology
   - wireless/mobile network security risks and safeguards
   - network addresses: physical/media access, reserved addresses; use of whois tools
   - domain naming and DNS
   - TCP/IP application ports: foundation for all network security and audit risk analysis
   - TCP/IP security risks and safeguards
   - security services: access control and encryption

3. Demystifying Network Media Access Technologies
   - network transmission media—twisted pair copper wire, fiber optics, wireless
   - network physical and logical topologies: bus, ring, star, tree
   - lan protocols ethernet, token ring, wireless LANS
   - geographical network delineation: PAN, LAN, CAN, MAN, WAN
   - physical WAN and internet connections: analog dial-up, leased lines, residential broadband
   - switched WAN network services: frame relay, ATM, MPLS
   - surveying wireless technologies, risks, and safeguards:

   - positioning network devices in the OSI Reference Model
   - interconnection devices: hubs, bridges, switches, routers, wireless access points—risks and safeguards
   - WiFi, bluetooth and WLAN security; risks and safeguards
   - network domains and segmentation
   - routers: border vs. interior routing protocols
   - network domains, virtual lans (VLANs) and segmentation
   - hierarchical network design implementation
   - network device maintenance/management port access security
   - simple network management protocol (SNMP)
   - enterprise authentication systems: TACACS+, RADIUS, diameter
   - network device security best practices for network interconnection device security and audit
   - network device audit procedures

5. Identifying and Managing Network Host Services Security
   - security control zones—developing a layered software risk analysis and management methodology
   - establishing your server security baseline
   - use of health check software tools and other analytical tools
   - port scanning—techniques and importance
   - server message block—risks and safeguards
   - managing and securing network file shares
   - managing and controlling remote control software—do’s and don’ts
   - network print and multifunction office devices—threats and vulnerabilities—risks and safeguards

6. Address Management and Directory Services Security
   - overview of critical network address management and directory services
   - manual and automated address management: hosts, DHCP, DNS, LDAP
   - domain name system (DNS)
   - lightweight directory access protocol (LDAP) directories
   - how to audit DHCP, DNS, LDAP and directory services

7. Effective Network Perimeter Security Strategies
   - perimeter security (hacker intrusion) objectives
   - network demilitarized zone (DMZ) architectures and key control points
   - network firewalls and proxy servers: policies, architectures
   - intrusion detection/prevention systems (IDS/IPS)
   - remote access/virtual private network technologies
   - how to secure VPN and remote access to your network
   - the risks of split tunneling
   - user authentication credentials
   - evolving nature of perimeter security threats
   - how to protect against phishing, spearphishing, credential theft, ransomware, malicious attachments, exploit kits and other techniques
   - analysis of landmark data breaches and strategies which would have prevented them

8. Wrap-up: Performing a Network Security Risk Analysis
   - identifying the network assets and control points
   - categorizing the threats and associated risks
   - vulnerability management: identifying, tracking, and closing serious network exposures
   - analysis of the first “cyberweapon”
   - a practical strategy for information security—12-point plan for success

SCHEDULE

December 9-11, 2019
Orlando, FL

April 27-29, 2020
Boston, MA

August 10-12, 2020
New York, NY

December 7-9, 2020
Orlando, FL

Available In-House (page 8).

Tuition $2395 24 CPEs
Web: misti.com/ASG203

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM
Cloud Security Fundamentals

How to Assess the Security of Your Cloud Solution

Seminar Focus and Features
This seminar will provide attendees with a comprehensive review of cloud technologies and cloud security fundamentals. The course covers all major domains identified in the guidance document from the Cloud Security Alliance (CSA), the Cloud Control Matrix (CCM) from CSA including mapping of controls to other various security frameworks, and the recommendations from the European Network and Information Security Agency (ENISA). Attendees will learn about key vulnerabilities in cloud solutions and strategies for managing those risks.

At the completion of this seminar attendees will:

- Identify security expectations for implementation of cloud-based solutions and fundamental cloud security principles and requirements
- Assess the overall level of security offered by cloud providers
- Build the necessary assessment processes for engaging with cloud providers

Prerequisite: Introduction to Information Security (ISG101) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Information Technology
Delivery Method: Group-Live

Who Should Attend
IT professionals; IT security professionals; auditors; risk management professionals; CISOs

What You Will Learn
1. Introduction to the Cloud
2. Cloud Service Categories and Deployment Models
3. Legal and Regulatory Concerns
4. Cloud Control Frameworks
5. Key Elements of Cloud Security
6. Data Security, Privacy and Encryption
7. Cloud Operations and Data Centers
8. Identity Management
9. Considerations for Office 365
10. Software Development Security Considerations for the Cloud
11. Business Continuity and Disaster Recovery Considerations for the Cloud
12. Top Threats to Cloud Computing
13. Incident Response
14. IT Governance or Cloud Computing, Managing the Risk
15. Auditing in the Cloud

Auditing Your Digital Presence

Assessing Your Virtual Marketing Efforts

Seminar Focus and Features
Digital marketing has transformed the consumer purchasing process. As your competitors adjust their marketing strategy to account for changing purchasing behavior, so should you. Never has it been more important for your digital content to be clear, concise, and most importantly—measurable.

In this three-day seminar we will dissect the challenges facing enterprises today and detail assurance activities your department can use to assess the effectiveness of the controls that safeguard today’s digital presence. By the end of this seminar attendees with have a better understanding of digital presence, the impacts of artificial intelligence and the role audit plays in assessing digital marketing efforts.

Prerequisite: Fundamentals of Internal Audit (OAG101), IT Audit School (ITG121) or equivalent experience
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Operational and IT auditors and audit managers preparing for an audit or self-assessment of their companies use of social media and other internet based marketing services

What You Will Learn
1. Defining Digital Presence
   - website
   - social media
   - email marketing
   - online advertising
2. What Artificial Intelligence Has to Do With Digital Marketing—“Predicting”
3. Features of Common Digital Marketing Platforms
4. What Is Adware and What Does It Do?
5. How Privacy Regulations Are Influenced by Marketing Efforts
6. Social Media Risks
7. Components of a Digital Presence Audit
   - inventory of digital presence (and your leading competitor)
   - business model/return on investment expectations
   - lead generation, outreach and closing deals
   - website analytics/”Google Analytics” search engine assessment
   - paid advertising ROI
   - content generation/marketing
   - social media marketing
   - APIs and how they drive customers to or away from sites “ease of use”
   - company website security: registration, access, administration, content, encryption
   - digital marketing cloud provider vendor assessment

SCHEDULE
Available In-House (page 8).
Tuition $2395 24 CPEs
Web: misti.com/ITG151

Virtual Classroom Available
Bold Dates Indicate Training Weeks

ZONE IS1
ISG207
ITG151
Information Security Boot Camp
Preparation for Common Body of Knowledge and (ISC)² CISSP Exam

Seminar Focus and Features
In this intense, information-packed five-day seminar, attendees will learn aspects of the (ISC)² Common Body of Knowledge (CBK) in conjunction with evaluating methods and tools required to construct or audit a comprehensive information security framework. You will gain a business-oriented, architectural perspective that defines how to organize and oversee a risk-based enterprise information security program, blending both theories and best management practices with key physical and information technology safeguards. To ensure attendees gain proper familiarity with industry leading practices, legislation and professional standards for information security, key references and yardsticks will be provided.

Attendees will be provided with unit and course review exercises and be able to return to their offices with the foundation of knowledge and know-how needed to take the CISSP exam (or similar), but even more importantly, to help guide their organization as it develops or revises its information security program.

Prerequisite: Introduction to Information Security (ISG101) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Information security and IT managers; information security analysts, architects and administrators; system administrators; network administrators; IT auditors; consultants; compliance managers; anyone needing a "crash course" in information security concepts and practices

What You Will Learn
1. Security and Risk Management
   • making the business case for information security
   • information security management objectives
   • risk analysis: threats, vulnerabilities, risks, and countermeasures
   • policies, standards, procedures, and guidelines
   • information classification
   • security awareness
2. Laws and Standards Affecting Information Security and IT Audit
   • computer crimes, investigations, evidence, forensics
   • laws, directives and regulations
   • types of laws
   • privacy issues and legislation
   • intellectual property, copyright laws and software piracy
   • European Union Data Protection Act
   • prominent US and international laws
   • information security and auditing standards
   • Security Engineering Security Concepts
   • Models, Mechanisms and Architectures
   • operating system security
   • virtualization: operational and security considerations
   • access control models, techniques and technologies, and methods
   • open and closed systems
   • security design standards and criteria: “Rainbow Series”, ITSEC, Common Criteria
   • certification and accreditation
4. Network Security Concepts and Solutions
   • defining a 3-layer simplified network protocol model
   • Open Systems Interconnection (OSI) model
   • network addresses and applications
   • LAN and WAN technologies, topologies and protocols
   • wiring: copper, fiber optics
   • wireless networks technologies, protocols and security
   • voice over IP (VoIP)
   • network interconnection devices: functionality, risks and safeguards
   • directory services: LDAP, DNS
   • network management tools: packet sniffers, SNMP, network utility and diagnostic software
   • network security vulnerabilities, threats, risks and countermeasures
   • hacker probing and attack techniques
   • firewalls and proxy servers
   • intrusion detection/prevention systems
   • VPNs and related Internet security protocols: SSL/TLS, IPSec, SSH
   • network discovery, vulnerability and penetration testing
5. Cryptography
   • demystifying the language of cryptography
   • key management: asymmetric, symmetric
   • encryption algorithms and hashing functions
   • digital signatures
   • Certificate Authorities (CAs) and Public Key Infrastructure (PKI)
6. Identity Management/Access Controls
   • authentication mechanism: passwords, tokens, smart cards, biometrics
   • point-to-point protocol (PPP) authentication: PAP, CHAP
   • extensible authentication protocol: EAP
   • enterprise authentication systems: RADIUS, TACACS+, Diameter
   • single/reduced sign-on (SSO): Kerberos, Web-based SSO
7. Software Development and Application Security
   • system development life cycle methodologies
   • configuration management and change control
   • application development tools and methodologies
   • client server and middleware security
   • data types and structures
   • Web application security architecture: control points, attacks and defenses
   • mobile code security risks: Java, ActiveX, JavaScript, VBScript
8. Asset Security (including Physical, Human Resources and Environment)
   • computing center location, construction and management
   • physical security threats, vulnerabilities, risks and countermeasures
   • perimeter security, boundary protection and facilities access controls
   • electrical, temperature, water, and other environmental controls
   • fire detection, prevention and suppression
   • information storage media protection, sanitization and disposal
   • human resources security: hiring practices, badges, terminations and transfers
9. Availability (Data Recovery and Business Continuity Planning)
   • business continuity planning requirements
   • business impact analysis
   • redundancy and fault tolerance
   • backup procedures: on-site and offsite
   • backup resources: processing sites, storage, offices, utilities, equipment and supplies
   • recovery testing procedures
   • emergency response procedures
10. Wrap-up Discussion

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM

SCHEDULE
December 9-13, 2019
Orlando, FL

June 15-19, 2020
New York, NY

September 14-18, 2020
Dallas, TX

December 7-11, 2020
Orlando, FL

Available In-House (page 8).

Tuition $3095 40 CPEs

Web: misti.com/ISG291
NIST Cybersecurity Framework
Guidelines and Best Practices for Managing Cybersecurity-Related Risk

Seminar Focus and Features
In today’s world, Cybersecurity is creating a lot of attention because of numerous breaches despite Cybersecurity legislation and industry-specific standards. Why is this continuing to be an issue for all businesses? The reason is simple; not one of the statutes, regulations or industry standards have integrated the all-important “Management System”.

Participants will take away valuable knowledge concerning the NIST CSF including developing a project plan and conformity matrix in addition to a roles and responsibilities matrix. By the end of the course, participants will have gained valuable hands-on implementation skills following a proven project management strategy.

Prerequisite: Introduction to Information Security (ISG101), Information Security Boot Camp (ISG291) or a general understanding of ISO 27001, risk management, audit, knowledge management, strategic business planning, communications, continual improvement

Advance Preparation: None

Learning Level: Intermediate

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Information security and network professionals including Chief Data Officers, Chief Information Security Officers and senior IT auditors wanting to gain a deep understanding of the Cybersecurity Management System Framework

What You Will Learn
1. Identify (ID)
   - Asset Management (ID.AM)
   - Business Environment (ID.BE)
   - Governance (ID.GV)
   - Risk Assessment (ID.RA)
   - Risk Management Strategy (ID.RM)
2. Protect (PR)
   - Access Control (PR.AC)
   - Awareness and Training (PR.AT)
   - Data Security (PR.DS)
   - Information Protection Processes and Procedures (PR.IP)
   - Maintenance (PR.MA)
   - Protective Technology (PR.PT)
3. Detect (DE)
   - Anomalies and Events (DE.AE)
   - Security Continuous Monitoring (DE.CM)
   - Detection Processes (DE.DP)
4. Respond (RS)
   - Response Planning (RS.RP)
   - Communications (RS.CO)
   - Analysis (RS.AN)
   - Mitigation (RS.MI)
   - Improvements (RS.IM)
5. Recover (RC)
   - Recovery Planning (RC.RP)
   - Improvements (RC.IM)
   - Communications (RC.CO)

NIST Cybersecurity Framework
Establishing a Repeatable Process for Managing Cyber Risk

Seminar Focus and Features
Since 2014 a large number of industries and special interest groups have created cybersecurity standards. All of these standard frameworks have been designed with a series of risk mitigating controls that are to be integrated into back off technology processes and front office business practices. Unfortunately to date all standard frameworks have failed to include a management system that would allow organizations to provide oversight including governance, risk management, internal audit, compliance management, continual improvement, communications, vulnerability management, incident management, awareness training, asset management, and continual management monitoring. Participants attending this course are going to leave with the skills necessary to initiate, plan, execute and control the adoption and integration of their own cybersecurity management system.

Prerequisite: Information Security Bootcamp (ISG291), Information Security Academy (ITG391), IT Risk Management School (ITG160), Conducting an IT Risk Assessment (ITG161)

Advance Preparation: General understanding of ISO 27001, risk management, audit, knowledge management, strategic business planning, communications, continual improvement

Learning Level: Intermediate

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Chief Data Protection Officers, Chief Information Security Officers, enterprise security program managers, internal audit directors, executives, Board of Directors

What You Will Learn
1. Understanding the Principles and Practices of Cybersecurity Governance
2. Protect (PR)
3. Defining the Cybersecurity Risk Management Process and Components
4. Assessing Opportunities for Continual Improvement of your Cybersecurity program
5. Defining and Exploring the Fundamental Components of a Cybersecurity Internal Audit Program
6. Developing a Cyber Program Communications Plan
7. Defining and Developing a Cybersecurity Training and Awareness Program

SCHEDULE
May 4-6, 2020
New York, NY
December 14-16, 2020
Chicago, IL

Available In-House (page 8).

Tuition $2395 24 CPEs

Web: misti.com/ISG370

SCHEDULE
February 24-27, 2020
New York, NY
October 5-8, 2020
Chicago, IL

Available In-House (page 8).

Tuition $2695 32 CPEs

Web: misti.com/ISG370
Security and Audit Considerations for Industrial Control Systems (ICS)

A Guide for Understanding Security and Audit Requirements of Industrial Control Systems

Seminar Focus and Features
This course is designed to assist auditors, examiners, operational technology and information technology professionals with understanding the essential elements of security for Industrial Control Systems (ICS) including Supervisory Control and Data Acquisition (SCADA). Through improving knowledge in this area, attendees will be better able to understand the risks facing this technology and provide assurances that organizational risks are appropriately mitigated.

ICS represents a growing concern as a cyber threat target. ICS technology often has a long life-span and the older systems in use today were not designed with cyber threats in mind. As more of these systems become network and internet connected to improve supportability and response, the potential to compromise these systems increases. Typically managed by operational technology staff, the security focus of these systems is availability first, followed by integrity then confidentiality; the reverse order from what information technology security focuses on (confidentiality, integrity then availability). Furthermore, since availability is the primary concern for these systems, artifacts and evidence of cyberattacks is often erased during the course of restoring system availability leading to a lack of visibility and reporting on this global threat.

Attendees will learn about the similarities and differences between information technology security and operational technology security, best practices in for operational technology security and how to develop ICS technology audit programs.

Prerequisite: Foundational knowledge of information security and audit for industrial control systems

Advance Preparation: None

Learning Level: Basic

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Information security professionals, IT auditors, IT management, operational technology professionals

What You Will Learn
1. Introduction to Operational and Information Technologies
2. Unique Threats to ICS Technologies
3. Case Studies
4. ICS Security Frameworks
5. Risks and Risk Management
6. Audit Considerations for ICS

Comprehensive Review of Critical Security Controls

Understand How to Implement the Highest Priority Security Controls

Seminar Focus and Features
This course provides a comprehensive review of the Critical Security Controls for effective cyber defense issued by the Center for Internet Security. These controls, developed and enhanced over the years by industry experts and the US military and other government entities, represent a risk-based and prioritized approach to cyber security. The controls lay out the consensus from respected industry experts as to the best way to block known attacks and the recommended approaches to find and mitigate damages resulting from successful attacks. Additional focus areas of this course include the applicability of these controls to Internet of Things (IoT), mobile technologies and privacy. Security professionals will gain an in-depth understanding of how to implement these controls; CIOs, auditor and risk management professionals will learn how to internalize these controls and assess their effectiveness in their organization.

At the completion of this seminar attendees will:
- Be able to incorporate critical security controls into their security program
- Be able to use the implementation of the critical security controls to lower organizational risk
- Be able to identify automated tools that can assist in implementing the controls

Prerequisite: Introduction to Information Security (ISG101) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
IT professionals; IT security professionals; auditors; risk management professionals; CISOs

What You Will Learn
1. Overview of Critical Security Controls
2. Common Attacks
3. Relationships Between Critical Security Controls and IT Governance
4. Critical Security Controls Review
5. Case Studies as Time Permits

Available In-House (page 8).

SCHEDULE
October 16-18, 2019
Chicago, IL

March 16-18, 2020
New York, NY

September 14-16, 2020
Dallas, TX

Tuition $2395 24 CPEs
Web: misti.com/ASN204
Information Security Academy
A Step-by-Step Guide to Establishing and Managing an Effective Information Security Program

Seminar Focus and Features
This four-day event will guide you through the basics of establishing and managing an information security program in today’s business environment. This class will cover internal and external threats, effective security policies, contingency planning, legislation, regulations, employee privacy issues, awareness programs and more. You will learn about emerging security architectural issues and technologies to assist you, how they can affect computer security in your organization, and what you can do to provide a secure environment even as technologies evolve. Participants will learn the components of a comprehensive plan, covering such critical areas as planning and managing a security program; getting the business more involved with information security; developing an enterprise security architecture; establishing identity and access control management and network perimeter protection; ensuring physical protection of your business and computing facilities, and complying with the legal and regulatory aspects of information security. The agenda will focus on risk analysis and business impact analysis (BIA) as tested methodologies for measuring the level of security risk and prioritizing information risk reduction in your organization. You are invited to bring your own information risk analysis evaluation criteria and targets, and explore how you can make best use of today’s techniques.

In addition, if you are auditing the security environment, this course will help you identify the essential elements that need to be developed and in place for your organization to maintain effective controls. Throughout the seminar videos, real-life scenarios and case studies will reinforce learning. You will leave this pragmatic course with a blueprint for building an effective information security program or for measuring an existing one.

Prerequisite: Introduction to Information Security (ISG101) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Information Technology
Delivery Method: Group-Live

Who Should Attend
Information security professionals with 5+ years of experience. Information security managers; newly appointed CISOs; IT managers; IT auditors; financial and operational auditors; business executives; risk managers; business continuity specialists.

What You Will Learn
1. Defining the Information Security Business Case
   - defining and delineating the attributes of an information security program
   - assessing threats to information security and areas of vulnerability
   - global legal and regulatory requirements for data protection and privacy
   - international requirements: SOX, Basel III and others
   - current concerns in information security
   - defining an enterprise information security architecture
   - changing views on information security
   - impact of cloud, dark data, etc.
   - NIST, CERT, FIRST, DISA and other great resources

2. Security Management: Strategic Components
   - defining the information security department charter
   - organizing for success: roles and responsibilities
   - the security management cycle
   - risk assessment and management
   - overall management vs. day-to-day administration
   - creating awareness programs
   - metrics, maturity models, and return on security investment
   - useful standards/guidelines for information security: ISO, IETF, COBIT, NIST/FISMA, NSA/ DISA, OWASP, ISF, SANS

3. Legislation and Standards
   - privacy protection laws
   - PCI DSS 3.1
   - anti-hacker legislation
   - emerging international security standards
   - common methods of identity theft
   - emerging law

4. Creating a Strong Foundation Through Policy
   - examining your environment and business drivers to create effective policies
   - tips for quickly creating policies
   - tools and techniques for examining your computing environment
   - case study/class exercises: developing organizational policies

5. Information Risk Analysis
   - the risk analysis cycle and its components
   - identifying assets in an information risk analysis
   - integrating risk management into an enterprise-wide process
   - partners in the information risk management process
   - types of information risk analysis: quantitative vs. qualitative approach
   - software tools for performing the information risk analysis process
   - identifying asset categories
   - defining information risk analysis targets and scope

6. Business Impact Analysis (BIA)
   - business impact analysis process: components and definitions
   - BIA as the key to a successful data security program
   - partners in the business impact process and their roles

7. Detecting Computer Crime, Accidents, and Errors
   - recognizing a computer crime/accident: identifying red flags
   - gathering and protecting evidence
   - creating a computer-crime task force: do’s and don’ts

8. Physical, Hardware, and Environmental Security
   - physical security
   - hardware security
   - media security
   - environmental controls in the distributed environment

9. Awareness Tools
   - methods for selecting effective tools, techniques, and trinkets
   - gaining management support
   - video examples and cost-effective sources for awareness

10. Business Continuity Planning (BCP)
    - defining the BCP management process
    - using the business impact analysis (BIA)
    - redundancy, backup, and fault tolerance
    - system and organization-wide recovery
    - plan management and testing

11. The Basics of Cryptography
    - understanding symmetric and asymmetric cryptography
    - crypto uses to protect data
    - future of confidentiality, integrity and identity/ authentication controls

12. The Future of Information Security in the Organization
    - management support
    - relating security to the business
    - nurturing the security and audit relationship
    - 12-point plan for success

SCHEDULE
October 28-31, 2019
Atlanta, GA
Tuition $2695 32 CPEs
Web: misti.com/ISG391

Available In-House (page 8).
Auditing Business Application Systems
A Step-by-Step Guide to Auditing How Applications' Transaction Activity, Controls and Procedures are Managed

Seminar Focus and Features
This two-day seminar is designed for financial, operational and information technology auditors who need to perform business application audits. Focusing on a top-down, risk-based approach you will learn how to assess key risks and controls in each stage of the application processing cycle and how to prioritize your audit approach to achieve optimal results in an effective and efficient manner. Discussions will include all aspects of a business application, including completeness and accuracy of input, processing and output.
You will learn techniques for identifying, prioritizing, assessing and evaluating application controls and procedures. You will leave the seminar with real-world examples of application control risks, control objectives, key application control assessments and testing techniques.

Prerequisite: IT Auditing and Controls (ITG101) or equivalent experience
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal audit staff, seniors and managers responsible for performing integrated internal audits, or those who want an introduction to IT Auditing.

What You Will Learn
1. Introduction to Business Application Systems
   - relationship between IT general & application controls
   - IT control categories
   - objectives of business application audits
   - types of business application audits
   - existing application reviews
   - end user computing
   - systems development audits
   - integrated auditing
   - data vs. information
2. Business Application Transactions
   - what is a transaction?
   - transaction-based application auditing
   - transaction life cycle
   - batch and online models
   - application risk assessment factors
   - establishing audit priorities
3. Top-Down Risk-Based Planning
   - planning the application audit
   - top-down risk-based planning
   - defining the business environment
   - determining the application's technical environment
   - performing a business information risk assessment
   - identifying key transactions
   - developing a key transaction process flow
   - evaluating and testing application controls
4. Executing Integrated Audits
   - control ownership
   - what is integrated auditing?
   - integrated IT/business controls
   - enterprise risk coverage
   - integrated audit staffing
   - COSO Principle 11—IT control activities
5. Business Application Controls
   - business applications—information objectives
   - business application auditing
   - business application transaction life cycle
   - transaction origination
   - completeness and accuracy of input; processing; output; master files; interfaces
   - output retention and disposal
   - data file controls
   - user review, balancing, reconciliation
   - end-user documentation
6. Testing Business Application Controls
   - testing business application controls
   - testing automated and manual controls
   - testing alternatives
   - testing sample size
   - sampling terminology
   - negative assurance testing
   - types of audit evidence
   - functional/substantive testing
   - Computer Assisted Audit Techniques (CAATS)
   - data analysis—planning and data verification
7. Documenting Business Application Controls
   - evaluating and documenting internal controls
   - internal control questionnaires (ICQ)
   - narratives
   - flowcharts/process flows
   - control matrix
8. End-User Computing
   - growth of end user computing
   - end user computing risks
   - general IT control risks
   - change control risks
   - purchased application risks
   - spreadsheets—typical errors
   - spreadsheet risk factors
   - practical steps for evaluating spreadsheet controls
9. Auditing System Development Projects
   - audit objectives
   - SDLC risks
   - primary reasons for problems
   - traditional system development life cycle
   - rapid application development
   - internal audit involvement

SCHEDULE
April 27-29, 2020
Boston, MA
July 13-15, 2020
Chicago, IL
October 19-21, 2020
New York, NY

Available In-House (page 8).
Tuition $2395 24 CPEs
Web: misti.com/ITG103

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM
Assessing the Risks of Bots and Disruptive Technologies

Risk Assessing and Auditing Disruptive Technologies That Are Driving the Future of Business

Seminar Focus and Features
This two-day seminar is designed to provide a basic understanding of the more progressive technologies that are expanding at a breakneck pace in the world of business. This course is designed to take a practical business-centric risk-based approach to understand the audit and risk implications of these technologies from a non-technical standpoint.

You will learn about the key risks and concerns that these advanced business tools create. We will cover the audit and risk assessment tactics that must be employed to assure that these strategic initiatives yield the high value returns that are anticipated. More importantly we will identify the significant risks that must be recognized, audited and dealt with to minimize any adverse impacts to the organization. Attendees will leave this seminar with an inventory of the key risks in these critical areas and the requisite audit knowledge to address each one.

Prerequisite: Risk School (OAR201), Data Mining for Auditors (OAP215) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Financial, operations, IT and regulatory auditors, public accountants, auditors in the public sector, audit managers and audit executives

What You Will Learn
1. Defining Artificial Intelligence (AI) and Related Sciences
2. Cognitive Automation
3. Disruptive Technologies (DT)—The Audit and Risk Issues
4. Blockchain
5. Risk Assessing and Auditing AI
6. Risk Assessing and Auditing Bots

SCHEDULE
July 16-17, 2020
Chicago, IL

November 16-17, 2020
New York, NY

Available In-House (page 8).

Tuition $2795 24 CPEs

Web: misti.com/OAR270

---

Successful Audit Data Analytics

Getting the Most Out of Your CAATs Program

Seminar Focus and Features
In this seminar designed for data analytics practitioners you will learn about effectively integrating data analytics or Computer Assisted Audit Techniques (CAATs), into an audit process. You will learn how to progress from basic analytics into a fully automated/repetitive mode, and learn the basics of continuous auditing. This seminar provides the opportunity to work on real-world scenarios with sample data files, and practice designing effective tests and critiquing and QA’ing the work of others.

As the course progresses, you will move from understanding basic analytic techniques such as stratifications, summarization and duplicate identification into more advanced techniques such as fuzzy matching, Benford’s Law and statistical and regression analysis. You will explore cutting-edge topics such as visual analytics, risk scorecarding and spatial analysis. Regardless of the tool you currently use or plan to use in your department—that generic audit-centric or more IT-oriented—the standard pseudo-code used throughout the course will allow you to easily take what you have learned and quickly code it in your tool of choice. Additionally, you will get hands-on experience working with demo versions of several popular tools, giving you the chance to see firsthand the strengths of each.

Prerequisite: Fundamentals of Internal Auditing (OAG101), IT Auditing and Controls (ITG101) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal and IT auditors, external auditors, business analysts and IT professionals looking to embed computer assisted audit techniques into their internal audit projects.

What You Will Learn
1. Integrating Data Analytics Across the Audit Process
2. Pros and Cons of Common Data Analysis Tools
3. Analytic Development Cycle
4. Planning Data Analytics Projects
5. Planning for Data Access
6. Advanced Analytic Design Techniques
7. Working with Standard Data Sources
8. Reporting and Interpreting Results
9. Developing Appropriate Standards
10. Making Analytics Repetitive and Continuous
11. Advanced Topics and the Evolution of Analytics
12. Common Analyses in Major Business Processes

SCHEDULE
October 14-16, 2019
New York, NY

December 2-4, 2019
San Francisco, CA

March 2-4, 2020
Denver, CO

May 18-20, 2020
Washington, DC

July 20-22, 2020
Atlanta, GA

September 14-16, 2020
Dallas, TX

Available In-House (page 8).

Tuition $2795 24 CPEs

Web: misti.com/ITP250
Fraud Data Analytics

Incorporating Data Analytics into Your Audit Program

Seminar Focus and Features
The best audit program in the world will not detect fraud unless the auditor selects the appropriate transaction for examination. Data analytics is the critical tool in locating and recognizing fraudulent activity in today’s core business systems. This course will combine fraud risk assessment and the use of data analytics to assist the auditor in responding to the risk of fraud within their audits. The course will demonstrate techniques that have located fraud that was hidden in company databases and focus on proven methodologies that will provide a framework to build your fraud analytics plan. This seminar will also show you how to build data interrogation search routines into your fraud risk assessment to locate data red flags.

Throughout the seminar, case studies and exercises will be used to reinforce the course material. At the conclusion of the seminar, attendees will build a data analytics plan to incorporate into their audit program and will be prepared to create search routines to uncover fraud in core business systems.

Prerequisite: Fraud Audit School (OAF201), Fraud Testing: Integrating Fraud Detection into Your Audit Program (OAF301) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal and IT auditors, external auditors, forensic accountants, corporate attorneys, risk management and information security personnel seeking to leverage and analyze quantitative data and improve the effectiveness of their fraud assessments and audits.

What You Will Learn
1. Introduction to Fraud Data Analytics
2. Data Mining Strategies
3. How to Build a Fraud Data Mining Plan
4. Data Analytics in Planning the Audit
5. Data Mining for Shell Companies
6. Data Mining for Fraudulent Disbursements
7. Data Mining for Corruption
8. Data Mining Company Credit Cards
9. Data Mining for Payroll Fraud
10. Data Mining for Theft of Revenue and Cash Receipts
11. Data Mining within the Financial Statements

SCHEDULE
December 9-11, 2019
Orlando, FL
April 27-29, 2020
New York, NY
September 14-16, 2020
Chicago, IL
December 7-9, 2020
Orlando, FL

Available In-House (page 8).

Tuition $2395 24 CPEs
Web: misti.com/OAF315

Fraud Testing: Integrating Fraud Detection into Your Audit Program

Asset Misappropriation: Locating and Recognizing Fraud Scenarios

Seminar Focus and Features
In this three-day seminar you will pinpoint the areas most prone to internal fraud and identify key indicators of fraud scenarios. The seminar content will cover the methodologies used by fraud auditors and focus on the red flags that signal the need for an investigation. You will focus on preparing fraud risk assessments for core business systems and integrating fraud detection into your audit program. You will learn how to implement and develop audit procedures that will increase the likelihood of discovering fraud, including fraud data mining. Throughout this seminar, case studies and class exercises will further illustrate how to integrate fraud detection into your audit program and reinforce proper fraud detection methodologies. At the conclusion of the seminar, you will be able to prepare a fraud risk assessment and integrate fraud audit procedures into your audit program.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or Fraud Audit School (OAF201) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Internal and IT auditors, external auditors, forensic accountants, corporate attorneys, risk management and information security personnel performing fraud assessments and audits.

What You Will Learn
1. Understanding How Fraud Occurs
2. Preparing the Fraud Risk Assessment
3. Business Process Fraud Risk Assessment
4. Integrating Fraud Detection into the Audit Program
5. Data Mining for Fraud
6. Fraud in the Disbursement Function
7. Fraud in the Procurement Office
8. Fraud in Payroll and Human Resources
9. Travel Expense Fraud
10. Fraud in Contracts
11. Fraud in Sales and Cash Receipts
12. Equipment and Asset Fraud
13. Money Laundering
14. Fraud Controls in Core Business Systems
15. Case Studies and Hands-on Exercises

SCHEDULE
December 16-18, 2019
San Francisco, CA
May 12-14, 2020
Chicago, IL
August 17-19, 2020
Boston, MA
December 14-16, 2019
New York, NY

Available In-House (page 8).

Tuition $2395 24 CPEs
Web: misti.com/OAF301

TO REGISTER  CALL 508 • 879 • 7999 EXT. 501  WWW.MISTI.COM
Data Mining for Auditors
A Logical Approach to Continuous Auditing and Governance

Seminar Focus and Features
In this extremely informative three-day seminar, we will cover all of the critical aspects of data mining that any auditor will need to know. You will understand key approaches that need to be taken when utilizing data to be effective. You will learn how to define which data should be used for what purposes to maximize the outcome of your audit efforts. You will learn the 10 commandments of data mining and how they must be applied to insure the success of each and every audit engagement. You will learn what is required to effectively and efficiently use proven data to maximize your value to the organization. But even more importantly you will learn how to realistically measure your value in real business facts that will be irrefutable proof of your contributions as an audit entity to the organization’s success.

If you don’t get ahead of the curve regarding the use of data in all of your auditing efforts, then by process of elimination you will be behind the curve. The audit functions that are truly world class and performing at maximum effectiveness are all data savvy and will dominate the practice of auditing at its highest level. You will leave this session thoroughly understanding the key ways to effectively determine the right data to use, and the right analytics to use it with in all of the right audit situations.

NOTE: Attendees are encouraged to bring a laptop to perform a number of exercises involving data and how it should be applied to your organization.

Prerequisite: Risk School (OAR321) or basic experience in using analytics in an audit setting
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Audit directors and managers, data analysts audit and risk, internal and external auditors, information technology auditors, and risk managers.

What You Will Learn
1. Aligning the Audit Function with the Business
2. Defining Data Mining & Continuous/Continual Auditing
3. Maximizing the Use of Data
4. Using Data Mining to Operate a Highly Effective Audit Risk Methodology
5. Data Analysis Methodologies: Focusing the Audits on Critical Business Concerns
6. Defining a Continuous/Continual Audit Process for Maximum Effectiveness
7. Rethinking the Audit Process
8. Focusing the Reporting on Outcomes Not Outputs

SCHEDULE
December 9-11, 2019
Orlando, FL
April 27-29, 2020
Boston, MA
September 14-16, 2020
Dallas, TX
November 2-4, 2020
Chicago, IL

Available In-House (page 8).
Tuition $2395 24 CPEs
Web: misti.com/OAP215

Root Cause Analysis for Internal Auditors
Strategies to Improve Internal Audit Recommendations and Uncover Why Controls Fail

Seminar Focus and Features
Whether an assurance or an advisory engagement, internal audit’s job is not done until we can explain why systems, processes and functional areas are not working as intended, Root Cause Analysis (RCA) uncovers what happened, why it happened and which changes need to be made. RCA approaches and techniques discussed and practiced in this two-day workshop should be part of every auditor’s toolkit.

This is a lively and interactive seminar will sharpen auditor analysis, communication and problem-solving skills. Participants will learn to apply the structured process of RCA to their audit practices. In addition, participants learn to balance creative and critical thinking at all five stages of RCA. Through many small group exercises, you will practice problem definition, collecting data, identifying possible causes, narrowing to root cause(s), and exploring solutions. We will discuss the risks and opportunities at each stage of RCA and explore new uses for traditional data collection methods. Prepare to be challenged to think differently and have fun!

Prerequisite: Fundamentals of Internal Auditing (OAG101) or Internal Audit School (OAP301) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
All levels of internal and IT auditors, from staff to CAE who want to improve their ability to identify, understand and document why issues happen in business processes.

What You Will Learn
1. Why Root Cause Analysis is Important to Auditing
   - three questions every audit should answer
   - relevant definitions and performance standards
2. Blocks to Effective Problem Solving
3. Analyzing Problems Thoroughly
   - three causal categories
   - five steps of root cause analysis
4. Gathering and Managing Data
   - identify sources of information to be analyzed
   - endeavor to include diverse points of view on the issues.
5. Pinpointing Cause and Effect
   - is/is not: transitional tool from data collection to cause identification
   - five whys
   - fishbone diagram
6. Identifying and Recommending Solutions
   - desired-result fishbone diagram
   - gather data/generating options
   - evaluating/analyzing options
7. Organizational Issues Related to Root Cause Analysis

SCHEDULE
April 30-May 1, 2020
Boston, MA
December 10-11, 2020
Orlando, FL

Available In-House (page 8).
Tuition $1995 16 CPEs
Web: misti.com/OAG223
Project Management for Auditors

Improving Audit Productivity with Project Management

Seminar Focus and Features
An audit is a project that requires planning, time, resources and a very specific set of skills. Subject matter expertise in auditing is not enough. This course challenges participants to consider what it truly takes to manage a successful project from start to finish. You will gain an understanding of the PMBOK’s five process groups and how they align with the audit life cycle. Individually and in small groups, participants will learn methods to improve their professional practices and results.

In two intensive days, participants will learn the fundamentals of project management, including how to achieve improved cost control, resource utilization and timelier audit conclusions. Participants will be involved in multiple hands-on exercises with selected tools and techniques. Using audit-specific examples, you will learn about project planning, scheduling, control and decision support concepts and methodologies. At the conclusion of the seminar, you will have solid tactics for managing time, increasing audit efficiency, driving a quality process, and producing quality deliverables.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Internal and IT audit staff, seniors, managers or senior managers responsible for the timely and comprehensive completion of an internal audit project.

What You Will Learn
1. Core Concepts and Definitions
   • project triangle: triple constraint on scope of work
   • three important themes
   • parallels to internal audit processes
   • ten knowledge areas in project management
2. Project Planning
   • how projects are initiated
   • guidelines, questions and tools
   • scoping, sequencing and scheduling
   • defining audit need, scope and stakeholders
   • identifying skills and requirements
3. Monitoring and Control
   • what is project control?
   • monitoring resources and deliverables
   • elements of good control
   • methods of gathering progress information
   • exercise: benefits and drawbacks of gathering methods
   • identifying attributes of good project information
4. Roles and Responsibilities of the Project Manager
   • importance of leadership in projects
   • communicating well
   • motivating others
   • rational and creative problem-solving techniques

SCHEDULE
October 24-25, 2019
New York, NY
March 12-13, 2020
San Francisco, CA
July 16-17, 2020
Chicago, IL
October 22-23, 2020
New York, NY
Available In-House (page 8).
Tuition $1995 16 CPEs
Web: misti.com/OAG211

Auditing Application Systems Development

A Step-by-Step Guide to Auditing Traditional and Advanced Applications Development

Seminar Focus and Features
In today’s organizations, audits of business application systems development are complicated by the presence of different computer platforms, a myriad of user needs and diverse technical environments. This three-day seminar, participants will explore proven audit strategies that will enable them to efficiently audit and evaluate applications systems development in a variety of technical environments. We will review common applications development risks, how to overcome them and what to do to meet the internal control and documentation requirements of SOX. Attendees will focus on what they need to know, what they need to do and when they need to do it. Attendees will leave this seminar with audit programs, questionnaires and sample audit findings to put to use as soon as they return to the office.

Prerequisite: IT Auditing and Controls (ITG101), IT Audit School (ITG121), or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Internal and IT auditors tasked with auditing the SDLC cycle or IoT development initiatives

What You Will Learn
1. Technical Environments and Their Impact on Application Systems Development
2. Preventing Application Systems Development Failures
3. The Impact of SOX
4. Common Challenges to All Methodologies
5. Implementing New Releases of Purchased Application Systems
6. In-House Application Systems Development
7. Web-Based Application Systems Development
8. Rapid Applications Systems Development
9. Auditing Applications Systems Design Specifications
10. Auditing Anticipated Application Internal Controls
11. Auditing Programming
12. Auditing Purchased Application Systems
13. Auditing Testing
14. Auditing Implementation and Change Control
15. Auditing Training
16. Auditing Computer Security
17. Conducting Post-Implementation Reviews
18. Application Software Inventory Control
19. Auditing Project Management
20. Getting Your Audits Done Faster
21. Auditing Rapid Application Development
22. Reporting Audit Findings
23. Planning for the Future
24. Automated Audit Tools
25. The Relationship Between Applications Development and IT General Controls in a SOX World

SCHEDULE
February 24-26, 2020
Orlando, FL
August 10-12, 2020
New York, NY
Available In-House (page 8).
Tuition $2395 24 CPEs
Web: misti.com/ITG212

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM
Using Risk Assessment to Build Individual Audit Programs
A Methodology That Addresses Management’s Business Concerns

Seminar Focus and Features
In this three-day seminar you will learn how to use risk assessment, generally applied to annual audit plans, to help build individual audit programs that will boost auditor productivity and confidence when they go to the field. You will explore the differences between traditional, control-based risk assessment and a new, business risk-based approach that addresses management’s concerns at the individual audit level. This progressive risk-based approach will demonstrate how assurance and consultative auditing can be performed simultaneously to maximize your audit resources and generate high-impact outcomes. You will learn how to recognize primary risks critical to any organization and to evaluate if there are appropriate controls in financial, information systems, compliance and operational audits. You will investigate the innovative methodology in a practical, real-world, audit-based work session that will take you step-by-step through the development of an individual audit program that was executed and the startling results. You will leave this session with a totally innovative approach to engagement-level risk assessment.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Risk School (OAR201) or equivalent experience
Learning Level: None
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and IT audit seniors, managers, senior managers and directors

What You Will Learn
1. Traditional Approaches to Risk Assessment
2. Information Sources Required to Truly Determine Risk
3. Maximizing Your Audits with Sound Data and Informed Judgment
4. A Business-Risk Approach to Value-Added Audit Programs
5. Focusing the Audit on Risk: A Multi-Level Approach
6. Risk Assessment in the Four Major Types of Audits
7. Maximizing Your Value: Talking Business Not Audit

SCHEDULE
March 2-4, 2020
Boston, MA

August 10-12, 2020
New York, NY

Available In-House (page 8).

Tuition $2395 24 CPEs
Web: misti.com/OAR321

Building a Continuous Risk Assessment Model
Utilizing GAS, Microsoft Office and New Systems Development Initiatives

Seminar Focus and Features
The number and intensity of emerging risks that organizations are experiencing are increasing at a mind-boggling pace, making the review and assurance process more difficult than ever. This two-day seminar will establish a framework for auditors to build a continuous risk assessment tool that will allow them to become leading-edge practitioners. You will learn the art of defining and building a highly effective methodology to identify the key risks facing the organization on an enterprise basis and how to define these risks in terms of Key Risk Indicators (KRIs). Discover how to ensure that all of these key risks are being actively evaluated on a continuous basis in order to maintain effective governance. You will also develop and optimize a dynamic risk-based audit plan that will keep the audit function in constant contact with the key risks of the organization to maximize effectiveness and coverage, while minimizing required resources. This is an interactive workshop requiring active participation in each of the key areas for participants to define, design and build each of the components to establish the basic components of a continuous/continual risk model.

NOTE: To ensure you get the most out of this seminar, you are encouraged to bring a laptop.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Risk School (OAR201) or equivalent experience
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live

Who Should Attend
Internal and IT audit managers, directors and CAEs; risk and compliance senior managers and executives

What You Will Learn
1. Establishing the Basics of Continuous/Continual Risk Assessment
2. Mapping the Organization—Understanding the Playing Field
3. Defining the Key Risk Parameters of the Model
4. Defining the Best KRIs for the Model
5. Combining the Tools to Build a Continuous/Continual Risk Assessment Environment
6. Utilizing GAS to Extract Key Data from Critical Systems
7. New Systems Development Strategies to Incorporate Continuous/Continual Risk Assessment

SCHEDULE
April 30-May 1, 2020
Boston, MA

September 17-18, 2020
Dallas, TX

October 22-23, 2020
New York, NY

Available In-House (page 8).

Tuition $1995 16 CPEs
Web: misti.com/OAR250
How to Audit IT General Controls
Exploring Common Techniques Used When Assessing IT General Controls

Seminar Focus and Features
Every internal auditor today must have a general understanding of technology and the vulnerabilities, threats and risks that face our enterprises each day to effectively plan and execute any audit engagement. In this three-day seminar, you will explore the IT general control areas that must be addressed to ensure confidentiality, integrity and availability as well as reliability and privacy of our sensitive and proprietary data and information assets. During this seminar, we will discuss the most common IT related vulnerabilities, threats and risks facing most enterprises today and the key controls to help reduce those risks to an acceptable or tolerable level.

We will explore critical aspects of the IT environment including the importance of data governance and data management, the scenario-based risk assessment process commonly used by IT risk managers and you will walk through many of the most common technologies and associated vulnerability, threats, risks and controls using common business language and using common applications as our examples. We will have several discussions examining various documents to allow attendees to apply the knowledge learned during the session. By the end of this session attendees will have a better understanding on how to plan, scope and conduct an IT general controls audit.

Prerequisite: Fundamentals of Internal Audit (OAG101), IT Audit School (ITG121) or equivalent experience
Advance Preparation: None
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Experienced IT auditors and technologists responsible for performing an IT general controls review audit or self-assessment.

What You Will Learn
1. Data and Information Governance and Management
2. Effectiveness of IT Governance
3. Common IT Control Standards and Frameworks
4. IT Risk Management Using Scenario Analysis
5. Technology Overview
6. Assessing Information Technology

Audit and Security for Cloud-Based Services
Security and Control Considerations for Cloud Computing Architectures

Seminar Focus and Features
In this two-day seminar you will explore the current state of cloud computing and its common architecture and examine the major SaaS, PaaS and IaaS providers in the market today. You will cover the security and control deficiencies that exist in cloud-based services and look at Security-as-a-Service as a way to protect against them. You will review a risk-based approach to audit and controls for cloud-based services and investigate such areas as cloud-based network models, cloud access security brokers, disaster recovery and governance in a cloud environment. This seminar will reinforce what you learn with real examples to help you identify the risks, controls and gaps in cloud services.

Prerequisite: A working knowledge of operating systems security, networking concepts and associated logical access controls; Network Security Essentials (ASG203); Intermediate IT Audit School (ITG241); or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Operational, business application, IT and external auditors; audit managers and directors; information security professionals.

What You Will Learn
1. Cloud-Based Computing: An Architectural Overview
   • the SPI Cloud Computing Model
   • NIST cloud model
   • key drivers for moving towards cloud-based services
2. Cloud Service Model = SPI
   • SaaS
   • transaction processing
   • other services
   • PaaS & aPaaS
   • IaaS
   • CSBs – Cloud Service Brokers
   • Security as a Service
3. Security Standards
4. Risk Assessment
   • business usage
   • data identification
   • NIST risk assessment process
5. Vendor Management
   • control frameworks
   • outsourcing risks
   • contracts and right to audit
   • certifications
   • security statements by provider
6. Internal Security
   • internal responsibility and

“Extraordinarily informative and understandable. Tom Salzman is an excellent instructor.”
Director
Macias Gini & O’Connell LLP
Securing and Auditing Windows® Active Directory Domains

Proven Strategies for Maximizing the Results of Your Windows Audits

Seminar Focus and Features
This four-day, hands-on seminar will focus on the skills required to effectively audit Active Directory. Using VMware workstations, each attendee will have their own virtualized Windows Server 2012 R2 Domain Controller and Windows 7 Workstation to put into practice the concepts and techniques learned during the class with a series of 15 hands-on labs. The output from each of the labs will be incorporated into an Excel spreadsheet that can be used as the basis for an audit program. Separate sheets in the Auditing Active Directory Excel spreadsheet summarize how to obtain Active Directory data using PowerShell scripts, items to look for in the output and a place to store samples of the PowerShell output. Attendees will be given their completed spreadsheet to take with them on a USB key along with the lab notes and PowerShell scripts.

The goal of this class is to develop a practical methodology for auditing and securing Active Directory. It will investigate attacks against Active Directory and how to protect against these attacks. Audit techniques covered are designed to make Active Directory exponentially more secure and difficult to hack. The last day of class will include a role playing exercise to put into practice the skills learned earlier in the class in a challenging real world auditing environment.

Prerequisite: A working knowledge of Windows Server, Windows 7, Excel and VMware Workstation is helpful, but not mandatory.

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
System and security administrators; infosec managers and analysts; network administrators; security architects; IT auditors; consultants.

What You Will Learn
1. Windows and Windows Networks
2. Auditing Active Directory Core Components
3. Auditing Active Directory Users
4. Auditing Active Directory Groups
5. Auditing Password Policies
6. Auditing Folder Rights
7. Auditing Active Directory Delegation
8. Security Compliance Manager and Group Policy
9. Auditing User Rights and Event Viewer Logs
10. Hardening Active Directory
11. Active Directory Case Study

Risk in Payment Systems

The Risks Associated with Change Including SWIFT, Cyber Currency, Blockchain and ACH

Seminar Focus and Features
Payment systems from ACH through blockchain and cyber currencies to Zelle and RTP are being provided to the marketplace at a fast pace and are changing the way we are working. This course looks at all the current developments and seeks to assist firms to understand what is happening, enabling them to consider their options. Focusing on the risks that are likely to arise in practice, this course is always amended for every event to ensure it reflects current developments.

By the conclusion of this course, delegates will have gained an appreciation of the controls, risks and options associated with SWIFT, CHIPS, ACH, Nested customers, blockchain and cyber currencies and cards as they develop.

Prerequisite: Bank Internal Audit School (OAP385) or equivalent experience. General knowledge of banking operations and retail/corporate banking products would be an advantage.

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend
Risk managers, executives, internal auditors, internal control staff

What You Will Learn
1. Risk and Governance
2. Fedwire, CHIPS and SWIFT
3. Mobile Financial Services
4. Newer Payment Types
5. ODFI and RDFI
6. Problem Areas
7. Same Day ACH
8. Card Issues
9. International Payments
10. Looking to the Future

SCHEDULE
November 4-6, 2019
Orlando, FL
May 12-14, 2020
Miami, FL
December 14-16, 2020
New York, NY

Available In-House (page 8).

Tuition $2695 24 CPEs
Web: misti.com/OAR225
Governance, Risk and Compliance
Real-World Solutions for Creating a Best-Practice GRC Framework

Seminar Focus and Features
It is a significant responsibility for an organization to implement and maintain a GRC Framework. Today's organizations have implemented selected components of a GRC framework, but the challenge still remains: Which strategies need to be implemented to have a completely integrated GRC approach? In this three-day, interactive seminar attendees will learn from a practicing CRO/CCO how to implement a best-in-class GRC Integrated Framework in an organization. Attendees will learn what the Audit Committee and boards are seeking from their executives about GRC. You will learn how to work with executive management to set the appropriate “tone” for ethics, compliance, investigations and fraud reporting, and the management of governance risks. Participants will learn how to successfully leverage every part of your organization to be part of the Chief Risk Office. You will also learn the steps to take to make the internal audit function a strategic part of the GRC framework. Attendees will be provided with the tools and best practices you need to implement an integrated GRC model in your organization.

NOTE: This seminar is continually updated to reflect the latest GRC hot topics.

Prerequisite: Advanced Auditing for In-Charge Auditors (OAG201), Managing the Internal Audit Department (OAM401) or equivalent experience
Advance Preparation: None
Learning Level: Advanced
Field: Auditing
Delivery Method: Group-Live

BONUS
Charters for the Ethics & Compliance Committee; Code of Ethics; Conflict of Interest Statement; Guidelines for consistent policies & procedures; Regulatory Compliance Playbook; Universe of Regulatory Areas to consider; Fraud Policy; Checklists for selected compliance areas; ERM Approach & Model; Roles & responsibilities of the Chief Risk Office; Pulling It All Together through Technology & Dashboard Reporting; Best practice GRC Framework "Snapshot"

Who Should Attend
Chief Compliance Officers, CAEs, Audit Directors and Managers; Chief Risk Officers and Chief Ethics Officers; internal and external auditors; anyone newly charged with GRC responsibilities.

What You Will Learn
1. GRC: First, Answering the Important Questions
   - what is it?
   - why is it important?
   - why are we here? The defining moments!
   - who is involved?
   - what are the roles and responsibilities?
2. Understanding Governance Risks: The GRC Model
   - different drivers in corporate governance
   - focus on “risks”: thinking like the CCO and CRO
   - the “four cornerstones” of a corporate governance framework: the board, executive management, internal auditors, and external auditors
   - The board and audit committee: stewards for governance reform
   - executive management and tone at the top

3. A Strategic Look: Expectations and Challenges in Building and Implementing the GRC Framework and Model
   - understanding your organization
   - what to expect: traditional roadblocks
   - impact of the organization's political environment
   - who should be the program sponsor and that person's role
   - making GRC a strategic objective for the organization

4. Analyzing the Tone-at-the-Top and Tone-in-the-Middle
   - what does tone at the top really mean? tone-in-the-middle?
   - who sets the tone at the top
   - how to assess and determine an organization's tone
   - performing a "quick tone at the top" assessment
   - dealing with a tone that is unacceptable

5. GRC - Four Key Components and Your Roadmap to Success
   - compliance and regulatory matters
   - ethics
   - investigations and fraud reporting
   - managing risks: levels 1 and 2
   - the diagnosis: outlining the important questions to ask
   - designing and executing the right program for your organization

6. Always Start with Risk: GRC Focus on Managing Risks
   - determining your tolerance to risk and your organization's objectives
   - establishing the ERM Program and required sponsorship
   - linking ERM to the annual planning process
   - defining level 1 and level 2 risks: a different application of the risk pyramid
   - adopting a risk culture
   - applying the risk process to major events: acquisitions and divestitures

7. Compliance and Regulatory Matters: The Core Strategy
   - forming the compliance committee and charter
   - assessing the impact of laws and regulations
   - the regulatory risk assessment
   - identifying and using your organization's subject matter experts

8. Ethics: Values and Behavior
   - forming the ethics committee and charters
   - establishing a code of ethics and business conduct
   - developing a separate and distinct conflict of interest statement
   - hiring ethical employees: what needs to be done
   - HR policies and procedures: what's important
   - performance appraisals
   - conducting ethics investigations

9. Investigations and Fraud Reporting: Standing Your Ground
   - establishing a fraud policy and an anti-fraud program
   - the fraud risk assessment
   - communication channels
   - the protocols for an effective investigation
   - evaluating controls and the connection to SOX

10. Key Strategy: Implementing the Chief Risk Office/Chief Compliance Office
    - defining the Chief Risk Office/Chief Compliance Office
    - the organization: who should be involved; roles and responsibilities
    - the connection to/working with operations, legal, accounting, IT, etc...
    - leveraging existing self-monitoring activities and infrastructure
    - evaluating the corporate governance program

11. Pulling It All Together
    - building a best in class compliance organization
    - SOX considerations: entity and transaction level
    - developing the “playbook”

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM
Managing the Fraud Audit Function
Integrating Fraud for a More Fraud Savvy Audit Department

Seminar Focus and Features
In this three-day session, you will obtain a comprehensive understanding of how to integrate fraud into your audit department's audit plan. Because fraud is a high-risk factor facing organizations, boards and chief executives are expecting auditors to detect fraud and be able to help management build anti-fraud programs. By applying the concepts to real-life fraud schemes occurring in today's business environments, you will learn to integrate fraud into your audit department, create fraud audit programs and help management mitigate the opportunities for fraud occurring in core business systems. You will leave this seminar with the knowledge to make your department more fraud savvy.

Prerequisite: Fundamentals of Internal Auditing (OAG101), Fraud Audit School (OAF201), or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Internal audit seniors, managers; senior managers; directors; vice presidents and CAEs with responsibility for integrating fraud into their audit plan.

What You Will Learn
1. Demystifying Fraud Risk
2. Managing the Organization's Fraud Risk Universe
3. How to Create Fraud Awareness
4. Vital Discussion Points with Your Audit Committee
5. Ensuring the Audit Department Has a Strategy for Responding to the Risk of Fraud
6. Using Fraud Risk Assessment to Build Your Fraud Audit Program
7. Strategic Plans for Implementing a Robust Fraud Data Analytics Plan
8. Managing Fraud Audit to Fraud Investigation
9. Understanding Statutory & Regulatory Requirements of the Fraud Risk Legislation
10. Critical Fraud Policies for Your Organization
11. Emerging Fraud Issues
12. Practical Audit Guidance for Specific Fraud Schemes

SCHEDULE
October 7-9, 2019
New York, NY

May 4-6, 2020
New York, NY

September 21-23, 2020
Washington, DC

Available In-House (page 8).
Tuition $2395   24 CPEs
Web: misti.com/OAF230

COBIT® 2019: Integrating COBIT into Your IT Audit Process
Utilizing COBIT 2019 for Planning and Executing Audits

Seminar Focus and Features
With the current emphasis on enterprise governance, successful organizations are integrating IT with business strategies to achieve their objectives, optimize information value and capitalize on today's technologies. To that end, COBIT, the internationally recognized set of IT management best practices, provides a powerful framework for IT governance, control and audit.

In this three-day seminar you will review the COBIT 2019 Framework and focus on how you can use this globally recognized framework for evaluating the effectiveness of IT activities. You will explore the significant changes incorporated in the new COBIT 2019 that can be utilized in executing IT audits. You will also discover how to use COBIT 2019 in conjunction with other internationally recognized standards and frameworks.

During the seminar you will explore examples using COBIT 2019 to plan and execute audits for IT governance, risk management, security management and business continuity. As a result of these exercises, you will fully understand how to use COBIT 2019 to provide a comprehensive and effective audit approach.

Prerequisite: IT Auditing and Controls (ITG101), IT Audit School (ITG121) or equivalent experience
Advance Preparation: None
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Anyone responsible for implementing or assessing IT and security controls. Internal audit seniors, managers and senior managers involved with identifying, assessing and reporting on technology related risks.

What You Will Learn
1. COBIT Background
2. Summary of COBIT 2019
4. Assessing IT Governance Using COBIT 2019
5. Risk Management
7. Manage Continuity
8. Integrating the COBIT 2019 Process Capability Model
9. COBIT Related Resources

SCHEDULE
April 30-May 1, 2020
Boston, MA

July 16-17, 2020
Chicago, IL

Available In-House (page 8).
Tuition $1995   16 CPEs
Web: misti.com/ITP241
**Auditing the Enterprise Risk Management Process**

Using This Critical Management and Governance Tool for a Top-Down, Risk-Based Approach to Mitigating Risk

**Seminar Focus and Features**
In this intensive three-day seminar you 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 has 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:** Risk School (OAR201) or equivalent risk assessment experience

**Advance Preparation:** None

**Learning Level:** Intermediate

**Field:** Auditing

**Delivery Method:** Group-Live

**Who Should Attend**
Audit directors and managers, risk officers, internal and external auditors, information technology auditors and operations managers

**What You Will Learn**
1. The Auditors Role in ERM
2. Developing an ERM Audit Process
3. Defining the Key Components of ERM
4. Defining the Key Components of Governance & Culture
5. Defining the Key Components of Strategy & Objective-Setting
6. Defining the Key Components of Performance
7. Defining the Key Components of Review & Revision

**SCHEDULE**
- October 21-23, 2019
  - New York, NY
- May 12-14, 2020
  - Washington, DC
- October 19-21, 2020
  - New York, NY

Available In-House (page 8).

**Tuition** $2395 24 CPEs

Web: misti.com/OAR341

---

**Audit Manager’s Guide to IT Risks**

Understanding Today’s Technologies and How They Impact the Organization

**Seminar Focus and Features**
New regulations, increasing IT security threats, evolving technologies and staff shortages challenge today’s audit executives to address the enterprise's increasing IT risks. To help avoid devastating harm to the organization's reputation from headline-making security breaches and address these IT risks, the IIA has issued advisories stating that ALL internal auditors must have sufficient knowledge of key information technology risks and controls (1210.A3); must consider the use of technology based and other data analysis techniques (1220.A2); and must assess information technology governance (2110.A2).

This two-day seminar is designed to help audit executives get up to speed on a wide range of technologies, meet the new challenges posed by technological change and provide assurance that IT risks are being adequately addressed. Presented in straightforward language, this briefing will provide you with a comfortable working knowledge of IT terms and concepts, update you on new and emerging technologies affecting your business and help you establish a strategic response to IT risks.

**Prerequisite:** Fundamentals of Internal Auditing (OAG101) or equivalent experience

**Advance Preparation:** None

**Learning Level:** Intermediate

**Field:** Auditing

**Delivery Method:** Group-Live

**Who Should Attend**
Internal audit seniors, managers and senior managers involved with identifying, assessing and reporting on technology-related risks for their internal audit projects or for the internal audit risk assessment.

**What You Will Learn**
1. IT Risks
2. Basics of Information Technology—Battling the Buzzwords
3. Logical Security Risks and Controls
4. Network Risks and Controls
5. Database Risks and Controls
6. IT General Controls
7. Auditing System Development Projects
8. Assessing IT Governance
9. Audit and Control Frameworks and Standards

**SCHEDULE**
- February 20-21, 2020
  - Orlando, FL
- June 9-10, 2020
  - San Francisco, CA

Available In-House (page 8).

**Tuition** $1995 16 CPEs

Web: misti.com/OAM302
LEADERQUEST CERTIFICATION COURSES
Specializing in cybersecurity training to support organizations’ evolving talent development needs

THE MISTI & LEADERQUEST ADVANTAGE

MISTI is proud to welcome LeaderQuest to its expanding portfolio of enterprise IT training solutions. Together we now offer a more complete learning ecosystem that spans from IT Audit risk assessment to IT networking operations to cybersecurity defense and certification. MISTI and LeaderQuest help organizations protect data and privacy, anticipate risks and defend business-critical systems and assets. We support your organization across the spectrum of IT audit, management, protection and readiness.

We serve the unique demands of your enterprise, offering virtual, instructor-led and live in-person training at our campuses in Denver, Dallas, Colorado Springs, Jacksonville and San Antonio. We will create customized, on-site training at your business location specific to your needs. We can create a tailored curriculum that includes certification and training across Cybersecurity, CISSP, CASP and CompTIA Security+... whatever your business environment demands.

MISTI’s acquisition of LeaderQuest will allow us to rapidly grow and expand through:
• Expanded domains - Cybersecurity and IT Networking
• New learning modalities - classroom, coursework, virtual, on-campus and client on-site
• Diversified enterprise audiences - IT Professionals, Veteran, Career Re-Training, Young Professionals & Job Recruiting

ABOUT LEADERQUEST

Since 2006, LeaderQuest has been a recognized leader in cybersecurity and IT training and job placement for military veterans, mid-career professionals and those seeking transitions to new career paths in information technology. Unlike other offerings, LeaderQuest’s entire training, certification and placement process takes only weeks - not years - enabling students to quickly begin or advance their careers in the field of IT and cybersecurity.

LeaderQuest is focused on creating an entire community of individuals empowered to pursue the tech careers they love by offering IT training and certification programs on the most relevant and in-demand technical skills for the future – including Network Support, Desktop and Computer User Support, System Administration, Database Administration, Front End Website Development with User Experience Design, Microsoft Web Development, Cybersecurity, and Project Management.

“We are delighted to be adding LeaderQuest to the MISTI platform. The LeaderQuest team has built a highly regarded and incredibly successful business model providing veterans and others career changers with the tools they need to enter the cybersecurity workforce, an area that is critically under resourced and in high demand.”

Tony Keefe, Chief Executive Officer
MISTI

“I am excited by the opportunities created as a result of uniting with MISTI and look forward to continuing to expand our core objectives. MISTI has a strong brand and reputation in the information security training industry and offers a platform that will allow us to broaden our audience across the globe.”

George Cohlmia, Chief Executive Officer
LeaderQuest

TO REGISTER      CALL 508 • 879 • 7999 EXT. 501      WWW.MISTI.COM
TAKE A LOOK

Explore our expanded portfolio of IT Networking and Cybersecurity training options below. We’ve taken the best that you have always known MISTI to deliver... and added the expertise of LeaderQuest’s Cybersecurity and IT Networking authority. Our expanded vision can offer your enterprise a unique training and business advantage.

For more information on the below course selections please visit www.leaderquestonline.com

ISC2 CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)
Learn to define the architecture, design, management, and/or controls that assure the security of business environments.

INTERCONNECTING CISCO NETWORKING DEVICES PART 1 (CCENT)
Learn how to install, operate, configure, and verify a basic IPv4 and IPv6 network.

INTERCONNECTING CISCO NETWORKING DEVICES PART 2 (CCNA)
Learn skills to install, configure, operate, and troubleshoot a small enterprise network.

PMP® IT PROJECT MANAGER PREP
Designed to help you pass the PMI® Certified Associate Project Management and Project Management Professional exams for the first time! Improve your test-taking skills while training for a great career!

COMPTIA ADVANCED SECURITY PRACTITIONER (CASP)
Build your skillset in enterprise security, risk management, incident response, and much more.

EC-COUNCIL CERTIFIED NETWORK DEFENDER (CND)
This course covers the protect, detect, and respond approach to network security along with the technical depth required to actively design a secure network for an organization.

EC-COUNCIL COMPUTER HACKING FORENSIC INVESTIGATOR (CHFI)
This course is a methodological training approach covering major forensic investigation scenarios that enable students to acquire hands-on experience on various forensic investigation techniques.

EC-COUNCIL CERTIFIED SECURITY ANALYST (ECSA)
Protect your organization by learning about modern infrastructures, operating systems, and application environments.

EC-COUNCIL CERTIFIED ENCRYPTION SPECIALIST (ECES)
This course introduces students to modern symmetric key cryptography including the details of algorithms such as Feistel Networks, DES, AES, Blowfish, Twofish, Skipjack, and others.

EC-COUNCIL CERTIFIED INCIDENT HANDLER (ECIH)
Learn how to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats.

EC-COUNCIL CERTIFIED DISASTER RECOVERY PROFESSIONAL (EDRP)
Creating a foundation for a career in IT support, networking, or cyber security

LeaderQuest is a CompTIA Partner, EC-Council Partner and AXELOS Partner
ITIL Foundation Training powered by LeaderQuest

Taking the First Step Into IT or Project Management

Seminar Focus and Features
Implementing and supporting IT services in the workplace can often be a daunting task since all organizations differ in key ways. Whether it's upgrading from one service to another, improving an existing service, or designing a service from scratch, business-focused leadership and management are crucial elements of services that your customers will perceive as valuable. This course will prepare you for the ITIL Foundation exam, introducing you to basic concepts used in IT service management. In this course, you will identify the fundamental concepts of ITIL to help prepare yourself for the Foundation Certification.

ITIL Foundation training and certification is a crucial fundamental class for anyone who uses IT services. Participants will be provided a practical understanding of key concepts, principles, processes, and functions to enable successful IT Service Management (ITSM) provision. This ITIL course will help individuals in aligning IT with business, controlling or reducing IT costs, improving IT service quality, and balancing IT resources in the most effective manner.

Based on the ITIL best practice service lifecycle approach, this course provides proven practical guidance and best practices on how to successfully introduce an integrated IT Service Management framework and how best practices can be adopted and adapted within an organization all while preparing you for the ITIL Foundations certification exam.

ITIL® is a registered trade mark of AXELOS Limited, used under permission of AXELOS Limited. All rights reserved.

Prerequisite: A basic understanding of the fundamentals of computers, networking, and security; should also be able to identify hardware, peripheral, networking, and security components.

Advance Preparation: None

Learning Level: Basic

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Indians looking to begin a career in information technology who want to gain the knowledge of networking, basic network security, and ITIL Foundation to provide any number of entry-level positions in desktop support, tech support, network support, and general IT support.

What You Will Learn
1. Define ITIL and its key concepts
2. Identify the components of the ITIL framework
3. Risk Assessing Interest Rate Risk Using Data Analytics
4. Analyze the ITIL guiding principles.
5. Identify the components and functions of the ITIL Service Value System (SVS).
6. Analyze the key ITIL management practices.
7. Define the general, service, and technical management practices of ITIL.

Day 1
Module 1: Introduction
Module 2: Service Strategy

Day 2
Module 3: Service Design

Day 3
Module 4: Service Transition

Day 4
Module 5: Service Operation Processes
Module 6: Service Operation Functions
Module 7: Continual Service Improvement

Day 5
Module 8: Continual Service Improvement

SCHEDULE

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 14-18, 2019</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>October 14-18, 2019</td>
<td>Colorado Springs, CO</td>
</tr>
<tr>
<td>October 14-18, 2019</td>
<td>Denver, CO</td>
</tr>
<tr>
<td>October 14-18, 2019</td>
<td>Jacksonville, FL</td>
</tr>
<tr>
<td>November 11-15, 2019</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>November 11-15, 2019</td>
<td>Colorado Springs, CO</td>
</tr>
<tr>
<td>November 11-15, 2019</td>
<td>Denver, CO</td>
</tr>
<tr>
<td>November 11-15, 2019</td>
<td>Jacksonville, FL</td>
</tr>
<tr>
<td>December 16-20, 2019</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>December 16-20, 2019</td>
<td>Colorado Springs, CO</td>
</tr>
<tr>
<td>December 16-20, 2019</td>
<td>Denver, CO</td>
</tr>
<tr>
<td>December 16-20, 2019</td>
<td>Jacksonville, FL</td>
</tr>
</tbody>
</table>

Available In-House (page 8).

Tuition $2295 45 CPEs

Web: misti.com/LIT101
**CompTIA A+ Core 1 Training powered by LeaderQuest**

The Foundation Needed for a Career in Cybersecurity and IT

**Seminar Focus and Features**

Whether working in a mobile or corporate environment with a high level of face-to-face customer interaction, where client communication and client training are important, or in an environment with limited customer interaction and an emphasis on hardware activities, this course provides the background knowledge and skills required to be a successful A+ technician.

This course continues with the Learn the basics of personal computer hardware and operating systems including installation, upgrade, repair, configuration, optimization, troubleshooting, and preventative maintenance. Participants will acquire the essential skills and information needed to install, configure, troubleshoot, upgrade, and perform preventive maintenance on PCs and mobile device hardware.

*To obtain your CompTIA A+ certification you must complete CompTIA A+ Core 1 and CompTIA A+ Core2 courses.*

**Prerequisite:** None

**Advance Preparation:** None

**Learning Level:** Basic

**Field:** Information Technology

**Delivery Method:** Group-Live

**Who Should Attend**

Individuals looking to start their careers in desktop support, computer user support, help desk tier I-III, and general IT support or are seeking to obtain the CompTIA A+ certification.

**What You Will Learn**

1. Support operating systems
2. Install, configure, and maintain operating systems
3. Maintain and troubleshoot Microsoft Windows
4. Configure and troubleshoot network connections
5. Manage users, workstations, and shared resources
6. Implement physical security
7. Secure workstations and data
8. Troubleshoot workstation security issues
9. Support and troubleshoot mobile devices
10. Implement operational procedures

**Day 1**

**Module 1:** Introduction

**Module 2:** Service Strategy

**Day 2**

**Module 3:** Service Design

**Day 3**

**Module 4:** Service Transition

**Day 4**

**Module 5:** Service Operation Processes

**Module 6:** Service Operation Functions

**Module 7:** Continual Service Improvement

**Day 5**

**Module 8:** Continual Service Improvement

**SCHEDULE**

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 21-25, 2019</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>October 21-25, 2019</td>
<td>Colorado Springs, CO</td>
</tr>
<tr>
<td>October 21-25, 2019</td>
<td>Denver, CO</td>
</tr>
<tr>
<td>November 18-22, 2019</td>
<td>Jacksonville, FL</td>
</tr>
<tr>
<td>November 18-22, 2019</td>
<td>Dallas, TX</td>
</tr>
<tr>
<td>November 18-22, 2019</td>
<td>Colorado Springs, CO</td>
</tr>
<tr>
<td>November 18-22, 2019</td>
<td>Jacksonville, FL</td>
</tr>
</tbody>
</table>

**Available In-House (page 8).**

**Tuition $2895**  
**45 CPEs**

**Web:** misti.com/LCA101
CompTIA A+ Core 2 Training powered by LeaderQuest

The Foundation Needed for a Career in Cybersecurity and IT

Seminar Focus and Features
This course is a continuation of CompTIA A+ Core 1. To obtain your CompTIA A+ certification you must complete CompTIA A+ Core 1 and CompTIA A+ Core 2 courses.

Whether working in a mobile or corporate environment with a high level of face-to-face customer interaction, where client communication and client training are important, or in an environment with limited customer interaction and an emphasis on hardware activities, this course provides the background knowledge and skills required to be a successful A+ technician.

This course continues with the basics of personal computer hardware and operating systems including installation, upgrade, repair, configuration, optimization, troubleshooting, and preventative maintenance. Participants will acquire the essential skills and information needed to install, configure, troubleshoot, upgrade, and perform preventative maintenance on PCs and mobile device hardware.

Prerequisite: CompTIA A+ Core 1 (LCA102)

Advance Preparation: None
Learning Level: Basic
Field: Information Technology
Delivery Method: Group-Live

Who Should Attend
Individuals looking to start their careers in desktop support, computer user support, help desk tier I-III, and general IT support.

What You Will Learn

1. Install and configure PC system unit components and peripheral devices
2. Install, configure, and troubleshoot display and multimedia devices
3. Install, configure, and troubleshoot storage devices
4. Install, configure, and troubleshoot internal system components
5. Explain network infrastructure concepts
6. Configure and troubleshoot network connections
7. Implement client virtualization and cloud computing
8. Support and troubleshoot laptops
9. Support and troubleshoot mobile devices
10. Install, configure, and troubleshoot print devices

**Day 1**
Lesson 1: Supporting Operation Systems
Lesson 2: Installing, Configuring and Maintaining Operating Systems
Lesson 3: Maintaining and Troubleshooting Windows

**Day 2**
Lesson 4: Configuring and Troubleshooting Networks
Lesson 5: Managing Users, Workstations, and Shared Resource

**Day 3**
Lesson 6: Security Concepts
Lesson 7: Securing Workstations and Data
Lesson 8: Troubleshooting Workstations Security Issues

**Day 4**
Lesson 9: Supporting and Troubleshooting Mobile Devices
Lesson 10: Implementing Operational Procedures

**Day 5**
Evaluation/Assessment/Assessment Review

SCHEDULE
October 28-1, 2019
Dallas, TX
Colorado Springs, CO
Denver, CO
Jacksonville, FL
December 2-6, 2019
Dallas, TX
Colorado Springs, CO
Denver, CO
Jacksonville, FL

Available In-House (page 8).

Tuition $2895 45 CPEs
Web: misti.com/LCA102
CompTIA Network+ Training powered by LeaderQuest

Advance Your IT Career with CompTIA Training and Network+ Certification

Seminar Focus and Features

The CompTIA® Network+® course will help build on existing user-level knowledge and experience with personal computer operating systems and networks to present the fundamental skills and concepts that will be needed on the job in any type of networking career. This course is designed to provide network technicians and support staff with the foundation-level skills they need to install, operate, manage, maintain, and troubleshoot a corporate network. This course will prepare you for CompTIA's Network+ certification, an ISO-17024 compliant, vendor-neutral technology certification that verifies the certified individual has the skills and knowledge needed to take on a pivotal role in building, managing, and protecting the critical asset that is the data network.

Prerequisite: While there are no required prerequisites for this course, CompTIA A+ is helpful

Advance Preparation: None

Learning Level: Basic

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend

Individuals who are working or looking to start their career as network technicians and support staff.

What You Will Learn

1. Identify basic network theory concepts and major network communications methods.
2. Describe bounded network media
3. Describe unbounded network media
4. Identify the major types of network implementations
5. Identify TCP/IP addressing and data delivery methods
6. Analyze routing and switching technologies
7. Identify the components of a TCP/IP implementation
8. Analyze network security
9. Implement network security
10. Identify the components of a WAN implementation
11. Identify the components used in cloud computing and virtualization
12. Identify the components of a remote network implementation
13. Manage networks
14. Troubleshoot network issues

Day 1
Lesson 1: Fundamentals

Day 2
Lesson 2: Physical Networks
Lesson 3: TCP/IP Networks

Day 3
Lesson 4: Internetworking
Lesson 5: Wireless LANs
Lesson 6: Wide Area Networks

Day 4
Lesson 7: Cybersecurity Principles
Lesson 8: Defending Networks

Day 5
Lesson 9: Evolving Network Technologies
Lesson 10: Network Operations
Lesson 11: Network Planning

Available In-House (page 8).

Tuition $2895 45 CPEs
Web: misti.com/LCN201
CompTIA Security+ Training powered by LeaderQuest

Expand Your Cybersecurity Career Through Certifications

Seminar Focus and Features
Cybercrime is on the rise and will more than triple the number of unfilled cybersecurity jobs in the coming years. Ransomware damages are predicted to exceed $5 billion dollars. Security+ certification will help participants increase their knowledge of these threats, attacks and vulnerabilities and prepare you on how to identify and prevent security threats. Over the course of this training participants will gain understanding of internals systems and services and internetwork devices and services. The CompTIA Security+ certification designates knowledgeable professionals in the field of security – one of the fastest-growing fields in IT!

Our CompTIA Security+ training will help you understand the field of network security and how it relates to other areas of information technology while preparing you to pass the current CompTIA Security+ certification.

Prerequisite: Basic computer literacy, PC operating system navigation skills, Internet usage skills and IP addressing knowledge are mandatory. CompTIA A+ and Network+ certifications or equivalent skills and knowledge are helpful but not mandatory.

Advance Preparation: None

Learning Level: Intermediate

Field: Information Technology

Delivery Method: Group-Live

Who Should Attend
Individuals who have a minimum of nine months of professional computer support experience as a PC or help desk technician.

What You Will Learn
1. Identify the fundamental components of information security
2. Analyze risk
3. Identify various threats to information security
4. Conduct security assessments to detect vulnerabilities
5. Implement security for hosts and software
6. Implement security for networks
7. Manage identity and access
8. Implement cryptographic solutions in the organization
9. Implement security at the operational level
10. Address security incidents
11. Ensure the continuity of business operations in the event of an incident

Day 1
Lesson 1: Understanding Attacks

Day 2
Lesson 2: Cryptography
Lesson 3: Network Fundamentals
Lesson 4: Securing Networks

Day 3
Lesson 5: Securing Hosts and Data
Lesson 6: Securing Network Services

Day 4
Lesson 7: Authentication
Lesson 8: Access Control

Day 5
Lesson 9: Organizational Security
Lesson 10: Disaster Planning and Recovery

SCHEDULE

October 14-18, 2019
Dallas, TX
October 14-18, 2019
Colorado Springs, CO
October 14-18, 2019
Denver, CO
October 14-18, 2019
Jacksonville, FL
November 11-15, 2019
Dallas, TX
November 11-15, 2019
Colorado Springs, CO
November 11-15, 2019
Denver, CO
November 11-15, 2019
Jacksonville, FL
December 16-20, 2019
Dallas, TX
December 16-20, 2019
Colorado Springs, CO
December 16-20, 2019
Denver, CO
December 16-20, 2019
Jacksonville, FL

Available In-House (page 8).

Tuition $2895 45 CPEs
Web: misti.com/LCS301
ACL Analytics is a tool that allows auditors and others to perform data analysis to gain greater insight into the accuracy and validity of corporate data by ensuring it was transacted in compliance with internal policies and procedures, and external regulations. It can also be used for purposes such as fraud detection, data scrubbing and data conversions.

Although auditors are the primary users, ACL Analytics is used for a multitude of analytic purposes. Anyone with data analysis needs can use ACL Analytics. Existing ACL Analytics users include:

- Auditors – Internal and External
- Fraud Examiners
- Operational Departments – Finance, Accounts Payable, IT, Production, etc.
- Most Industries – Manufacturing, Airlines, Retail, Insurance, Banking, Healthcare, Utilities, etc.
- Companies of all sizes – includes Fortune 100 and 500, Global 500, etc.
- Government Agencies – Federal and State

ACL users can now attend instructor-led, open-enrollment and in-house training classes delivered regionally for all user levels by experienced instructors with 20 years’ experience teaching and using ACL.

Stay up-to-date and informed! We have recently invested in bringing all courses up to date for 2019 to deliver you the most in-demand and timely content.
A Comprehensive Introduction to ACL™ Analytics

Everything You Need to Know to Start Being Productive with ACL Analytics

Seminar Focus and Features
This three-day ACL certified course introduces new and beginner users everything they need to know to start being productive with ACL Analytics. In an interactive, hands-on environment, your instructor, who has many years of ACL and audit experience, will start by teaching you the necessary fundamentals in less than half a day. The course will then build on the fundamentals and guide you through the typical data analytic phases of importing data, preparing data, analyzing data and reporting your results. On the third day, basic scripting will be introduced to demonstrate how easy it is to automate analytic routines with ACL Analytics.

Throughout this comprehensive introduction and practical application via instructor-led sessions and activities, you will learn how to effectively use ACL Analytics to accomplish your audit and/or business objectives. This is a highly interactive course where you are encouraged to ask for assistance, advice and guidance.

Prerequisite: PC and Windows experience
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
New and beginner users. This is a very thorough introduction, so it is the best way to get started with using ACL. Self-taught users often attend the course to learn what self-study cannot accomplish.

What You Will Learn

1. Basics
   - data concepts
   - ACL Analytics – environment and user interface
   - best practices
   - phases of data analysis

2. Expressions
   - expression overview
   - filters
   - word searches
   - computed fields–unconditional and conditional
   - function overview

3. Importing Data
   - locating and acquiring data
   - importing fixed width files
   - importing delimited files
   - importing excel files
   - importing print image report files
   - importing pdf files
   - importing via ODBC
   - re-using prior import statements

4. Preparing Data
   - understanding integrity
   - testing for validity (corrupt data and correct field definitions)
   - testing for controls
   - testing for date and character bounds
   - testing for quality and completeness
   - testing for missing items
   - testing for duplicates
   - testing for reasonableness
   - testing for calculation errors

5. Analyzing Data
   - grouping data (identifying category totals and trends)
   - reordering (sorting) records
   - isolating data (creating data file sub-sets to improve efficiency and track results)
   - combining data (stacking common files on top of each other and linking files on one or more common key fields)

6. Reporting
   - creating documentation reports for working papers
   - printing reports
   - exporting to other file types, such as Excel
   - how to access ACL’s GRC results lite module where exceptions can be tracked, distributed and monitored.
   - visualizing results in graphs

7. Scripts
   - introduction to automating analytic routines with scripts
   - working with variables to allow scripts to run against future data
   - scripting interactions that prompt for user input when a script is run

“The content, instructor, and exercises were fantastic, and I plan on coming back for the scripting class next year.”
Risk Control Service
TCF Financial Corporation
Functions and Case Studies within ACL™ Analytics
A Practical Application of ACL Analytics Using Real-Life Situations

Seminar Focus and Features
This two-day course is a practical application of ACL Analytics, designed to make you more effective in real life situations. The course commences with a presentation of functions for harmonizing, searching and converting data to assist with issues and questions that are frequently encountered when performing data analytics. You will gain hands-on experience and real-world explanations for using these functions as your ACL Certified Trainer leads you through this presentation. You will then be guided through three hands-on case studies (approximately half-day duration each) which will help you develop your critical thinking skills as you cleanse dirty data, prepare for analysis, perform multiple analysis objectives and report your results. You will learn how to document your approach by effectively separating objectives into manageable milestones that will make it easier to determine which ACL command, expression or function should be used. This documented approach will provide essential support to your working papers.

This course will also prepare you for level 4 of the ACL Certified Data Analyst (ACDA) exam.

Prerequisite: A comprehensive introduction to ACL Analytics (ACL101) or self-taught to a comparable level
Learning Level: Intermediate
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Those who have attended the ACL101 course or are self-taught to that level and require practice in applying ACL to typical data analytic scenarios, including further understanding in the use of functions to cope with typical objectives.

What You Will Learn
1. Review
2. Functions
3. Case Studies

SCHEDULE
October 24-25, 2019
Burlington, MA
November 21-22, 2019
Philadelphia, PA
December 19-20, 2019
Houston, TX
January 30-31, 2020
Las Vegas, NV
February 27-28, 2020
Atlanta, GA
March 12-13, 2020
New York, NY
April 9-10, 2020
Dallas, TX
May 21-22, 2020
Chicago, IL
June 11-12, 2020
Dublin, OH
July 16-17, 2020
Washington, DC
August 20-21, 2020
New York, NY
September 24-25, 2020
San Francisco, CA
October 22-23, 2020
Burlington, MA
November 19-20, 2020
Philadelphia, PA
December 10-11, 2020
Houston, TX
Available In-House (page 8).
Tuition $1650 16 CPEs
Web: misti.com/ACL201

Scripting with ACL™ Analytics
Create Simple and Interactive Scripts to Implement Automated Routines and Continuous Monitoring

Seminar Focus and Features
This three-day course provides a comprehensive introduction to scripting with ACL Analytics. In an interactive hands-on environment, you will learn scripting basics and best practices to provide you with the essential scripting foundations. You will then be shown how to script the import, preparation and analysis phases of an audit to create continuous routines that can be run against future data. In addition to scripting commands that exists within the user interface, you will also be taught how to leverage functionality that is only available to a script, such as the GROUP and LOOP commands, flag and counter-based loops and creating a script that creates another script. These features will add amazing power to your knowledge base. You will also see how functions play a vital role in the scripting process.

Throughout this comprehensive scripting course via instructor led sessions and activities, you will learn how to effectively use ACL Analytics to accomplish your scripting goals. This is an interactive environment where you can ask for assistance, advice and guidance. The thoroughly documented training manual will be used throughout the course and will provide you with essential future reference. You will also be able to take home with you the course training files, including all your class work and some pre-written scripts for routines such as cleansing addresses, split transactions, keyword searches and deleting temporary tables.

This course will also prepare you for level 6 & 7 of the ACL Certified Data Analyst (ACDA) exam.

Prerequisite: A Comprehensive Introduction to ACL Analytics (ACL101) or self-taught to a comparable level
Learning Level: Advanced
Field: Auditing
Delivery Method: Group-Live
Who Should Attend
Users who have completed the ACL101 course (or are self-taught to that level) and have been using ACL to the extent that they are comfortable using the ACL101 content. Attending the ACL201 course is not a prerequisite, but many users find it useful.

What You Will Learn
1. Basics
2. Importing Data
3. Preparing Data
4. Analyzing Data
5. Pre-written Scripts
6. Conclusion

SCHEDULE
November 18-20, 2019
Philadelphia, PA
December 16-18, 2019
Houston, TX
February 24-26, 2020
Atlanta, GA
Available In-House (page 8).
Tuition $2200 25 CPEs
Web: misti.com/ACL303
Anthony J. Bellezza, CPA, Independent Advisor and Senior Faculty Member, MISTI

Mark E.S. Bernard, CISSP, CISM, CISA, CGEIT, CRISC, Chief Executive Officer, Secure Knowledge Management

Steve Biskie, CISA, CITP, CPA, CGMA, Director, National Data Analytics Leaders & SAP Champion, IT Assurance, RSM US LLP

Jason D. Claycomb, CISA, CISSP, Founder, INARMA LLC

Dennis Cox, BSC, FCA, FISI, Founder & Chief Executive of Risk, Reward Ltd.

Kathleen Crawford, Senior Consultant, MISTI

Ken Cutler, CISSP, CISA, CISM, Q/EH, Security+, President & Principal Consultant, Ken Cutler & Associates InfoSec Assurance

Greg H. Duckert, CRMA, CRISC, CPA, CISA, CIA, Founder, Virtual Governance Institute LLC; Sr. Consultant, MISTI

Mark T. Edmead, MBA, CISA, CISSP, IT Transformation Consultant, MTE Advisors; Senior Instructor, MISTI

Shawna M. Flanders, CRISC, CISM, CISA, CSSGB, SSBB, Director of Instructional Technology & Innovation, MISTI

Martin H. Green, Esq., Senior Instructor, MISTI

Jeffrey T. Hare, CPA, CISA, CIA, CEO, ERP Risk Advisors

Peter Higgins, CIA, CRMA, Principal Consultant/Trainer, Boston Audit Solutions Group

Lane Paige Hollis, MBA, CPA, CFF, Corporate Manager, Internal Audit, Jacobs Engineering

Stephen Kost, Chief Technology Officer, Integrihy Corporation

Joel F. Kramer, CPA, Managing Director, Internal Audit Division, MISTI

Robert McDonough, CRP, CIDA, Senior Consulting Mgr., Angel Oak Consulting Group; Pres. & CEO, Strategic Financial Solutions, Inc.

Dr. Hernan Murdock, CIA, CRMA, Vice President, Audit Division, MISTI

Charles V. Pask, CISSP, M.Inst.ISP, Managing Director, ITSEC Associates Ltd

Keith Pennifold, ACDA ACL Certified Master Trainer and Data Analyst

Tony Redlinger, CIA, CISA, CISSP, CFE, Senior Manager, Internal Audit, IHS Markit

Rita C. Roberts, CISA, ACDA Managing Director, Analytical Support, LLC

Fred C. Roth, CISA, Senior Instructor, MISTI

Thomas Salzman, CISA, ITIL, IT Audit Manager, Illinois State University

Mary G. Siero, CISSP, CISM, CRISC, Information Technology Consultant

Alan Sugano, President, ADS Consulting Group, Inc.

Sarah Swanson, Trainer, Writer and Owner, Tumbleweed Consulting

Jim Tarantino, CISA, CRISC, ACDA, Client Solutions Director, High Water Advisors

Richard H. Tarr, CIA, CISA, Audit & Information Systems Consultant & President, Richard Tarr and Associates

John Verver, CPA, CISA, CMC, Global Director of Analytics Strategy, High Water Advisors

James Vogt, CFE, MS, CEO & Founder, Fraud Protection Institute

Leonard W. Vona, CPA, CFE, CEO, Fraud Auditing, Inc.

Tom Winson, Consultant, RSM US, LLP

To learn more about our esteemed faculty, please visit: www.misti.com/faculty
REGISTRATION INFORMATION

TO REGISTER CALL 508 • 879 • 7999 EXT. 501 WWW.MISTI.COM

Connect With Us

Online www.misti.com
E-mail customerservice@misti.com
Mail MIS Training Institute, 153 Cordaville Road, Suite 200, Southborough, MA 01772-1834
Call (508) 879-7999 ext. 501 Fax (508) 787-0033

Tuition
Tuition is listed after each course outline. Tuition covers admission, course materials and refreshments. Tuition is payable in advance by cash, company check (US dollars), VISA, MasterCard, AMEX, Discover or Diners Club.

Class Hours
MISTI seminars are conducted from 8:30 AM - 5:00 PM daily. Three, four and five-day classes conclude at 3:00 PM on the last day. Two-day classes conclude at 3:30 PM on the second day. Virtual Classroom seminars are conducted in the time zone of the host city. All ACL certified courses are group-live and are conducted from 8:30 AM - 4:30 PM daily. Class hours are subject to change. Please reference our website or call our Customer Service Department to check the hours for specific seminar dates.

Discounts
• Save 10% when registering three or more people for the same seminar on the same date.
• Attend consecutive seminars in the same week and save 10% on both seminars.
• Government: Take 10% off regular fees.
• Call Customer Service for more details on discounts.
(Savings do not apply to already discounted seminars, registrations must be made and paid for at the same time, and individual webinars or self-study online training and cannot be combined.)

Corporate Savings
PERC Preferred Education Rate Contract
Save 10-20% on public training;
PERC is a discounted volume training program designed to accommodate staff who require training in different areas.

How It Works
Your organization is billed in advance for the entire PERC amount, less the appropriate discount.* Throughout the year, you will receive training reports indicating how, where, by whom your PERC dollars have been used and how many PERC dollars remain in your account. For more information on PERC, call Customer Service at (508) 879-7999 ext. 501.

<table>
<thead>
<tr>
<th>PERC Dollars</th>
<th>Discount Rate</th>
<th>You Pay</th>
<th>You Save</th>
</tr>
</thead>
<tbody>
<tr>
<td>$15,000</td>
<td>10%</td>
<td>$13,500</td>
<td>$1,500</td>
</tr>
<tr>
<td>$20,000</td>
<td>15%</td>
<td>$17,000</td>
<td>$3,000</td>
</tr>
<tr>
<td>$30,000</td>
<td>20%</td>
<td>$24,000</td>
<td>$6,000</td>
</tr>
</tbody>
</table>

For information about programs in Europe, Middle East, Africa and Asia Pacific:
Phone +44 (0)20 3819 0800 E-mail misti@misti.com

Facility/Hotel Information
MISTI’s research has shown that our attendees training experience is enhanced when we have the opportunity to “right-size” their training room based on the expected number of participants. This ensures the comfort of all attendees and a positive learning experience! For this reason, attendees may not receive the information on their seminar training facility until approximately 4-6 weeks prior to the seminar. When facilities are assigned our attendees are notified and our website is updated. Should you prefer to book accommodations at other area hotels prior to that time, please feel welcome to do so. All hands-on events are held at MicroTek facilities, which provide hotel recommendations near their sites.

Schedule Changes/Cancellations
MISTI makes every effort to run all of the scheduled programs as advertised. In the instance that MISTI does cancel or reschedule an event we will give you as much advance notice as possible. Your tuition fee can be either held on account or refunded if MISTI cancels the event. MISTI is not responsible, however, for penalties incurred as a result of discount hotel reservations or air fare purchases. If you can no longer attend a training, please review the MISTI cancellation policy found on our FAQs page of our website, www.misti.com/ faqs and provide written notice to MISTI Customer Service at customerservice@misti.com. Cancellation policies are subject to change without notice.

CPE Credits
All participants are eligible to receive NASBA certified CPE Credits to fulfill professional accreditation requirements. Any extended absences from class may result in reduced CPEs earned.

High-Yield/No-Risk Guarantee
Attend a MISTI seminar and receive tools and techniques that will help you do your job better. If you do not, simply tell us why on your company letterhead within 30 days of attending the event and we will give you a full credit toward another seminar. Address your comments to MIS Training Institute, 153 Cordaville Road, Suite 200, Southborough, MA 01772-1834, or call (508) 879-7999 ext. 501.

MISTI is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be submitted to the National Registry of CPE Sponsors through its website: www.nasbaregistry.org

MIS Training Institute, 153 Cordaville Road, Suite 200, Southborough, MA 01772-1834, or call (508) 879-7999 ext. 501.
Mailroom: If undeliverable to addressee, please forward this catalog to Audit/Information Security personnel.

Duplicates: Because MISTI rents other mailing lists, sometimes duplicate catalogs mailed to one person are unavoidable. Please pass extra catalogs on to someone who might benefit from training opportunities. If you wish to have your name removed from the MISTI mailing list, send, email or fax us your mailing label. You can also contact our Customer Service Department at 508-879-799 ext. 501

IMPORTANT: Please refer to the Registration Code below when registering online or by phone.

Registration Code: A819/PDF