2017
COURSE CATALOG

SEPTEMBER 2016 - DECEMBER 2017

MIS|TI™
TRAINING INSTITUTE

WWW.MISTI.COM

"I thought this course was excellent. I got a lot of take-aways from this course as well as many meaningful ideas, which is exactly what I was hoping for."

Chuck Watson, CAE, General Audit, ASARCO

SPECIALIZED TRAINING IN

AUDIT + IT AUDIT + INFO SECURITY

A Letter From the CEO

As our global reach expands, we continue to pride ourselves in delivering world-class training to professionals, like you, in the audit, IT audit and information security fields. The importance of the duties that fall into these professions continues to grow as enterprises increasingly become technologically complex.

As talent shortages impact organizations around the world, audit and security professionals look to us to continue to acquire knowledge through our seminars, and network with industry leaders at our conferences across the country. Although our events and training services are at the core of our mission, we've embarked on a new journey that further provides value to our audience.

This initiative focuses on supporting our training efforts by playing off of the current up-to-the-minute topics that our core services are aimed at. Through relevant, timely and enjoyable content provided on our site and via our social media channels, you can now access an abundant source of insights that encourage you to not only think about problems differently, but also pursue opportunities.

Our mission has always been, and will always be, to arm internal audit, IT audit and information security practitioners with the knowledge they need to tackle the challenges that matter most. Conferences like SuperStrategies and InfoSec World are perfect examples of the opportunities we provide. But now, we're taking things one step further by consistently connecting with you and your peers to inform you via the devices you're attached to most.

This is a very exciting time for MISTI. I am looking forward to fulfilling our goals of building on our long-lasting relationships with our audience through physical events, and continuing the trend through interacting with you as both an attendee and a consumer of our digital content. I welcome your ideas and feedback as we grow the quality and value of MISTI's offerings.

Cheers!

Tony Keefe
President & CEO,
MISTI

Earn CPE Credits

By attending our seminars and events, you may earn up to 40 NASBA Certified Continuing Professional Education credits (CPEs) and related credits from many professional associations worldwide. See each individual seminar page to find out the specific number of credits for each seminar.

MISTI™ TRAINING WEEK

MISTI's Training Weeks bring you our most timely and in-demand courses in one information-packed week. Held in our most popular seminar cities across the U.S., this unique format provides a wide array of our top courses for you and your colleagues to choose from to maximize your learning and networking experience.

Two budget-trimming ways to save:

- Register three or more people from the same company in the same Training Week and save 10% on all three registrations
- Attend a two-day and three-day seminar during the same Training Week and receive a 10% discount

Attend a MISTI Training Week and you will:

- Maximize your travel budget while earning more CPEs
- Benefit from maximum one-on-one time with your instructors
- Spend a week in the company of colleagues who share your concerns and challenges
- Expand your network as you get to know your fellow attendees
- Learn from hands-on experts eager to share their expertise

Upcoming Training Weeks

Chicago, IL: September 19-23, 2016
New York, NY: October 17-21, 2016
Orlando, FL: December 12-16, 2016
San Francisco, CA: February 6-10, 2017
Las Vegas, NV: March 13-17, 2017
Boston, MA: April 24-28, 2017
Washington, DC: May 15-19, 2017
San Diego, CA: June 5-9, 2017
New York, NY: June 12-16, 2017
Boston, MA: July 17-21, 2017
Washington, DC: August 7-11, 2017
Anaheim, CA: August 21-25, 2017
Chicago, IL: September 25-29, 2017
New York, NY: October 23-27, 2017
Orlando, FL: December 4-8, 2017

Visit misti.com/TrainingWeeks for a complete list of dates. Training Week dates are indicated in bold throughout the catalog.

Upcoming Events

SuperStrategies 2016
September 27-29, 2016
Mirage Resort & Casino
Las Vegas, NV
superstrategies.misti.com

Co-Located Events

ITAC 2016
December 6-8, 2016
JW Marriott New Orleans
New Orleans, LA
ITAC.misti.com

Threat Intelligence Summit 2016
December 6-7, 2016
JW Marriott New Orleans
New Orleans, LA
threatintelligence.misti.com

More 2017 Events Coming Soon!
Keep up to date at www.misti.com

2017 Events

InfoSec World 2017
April 3-5, 2017
Omni Orlando Resort at ChampionsGate
ChampionsGate, FL
infosecworld.misti.com

Audit Directors' & Managers' Symposium
May 9-11, 2017
Sonesta Resort
Hilton Head Island, SC
www.misti.com/OAM500

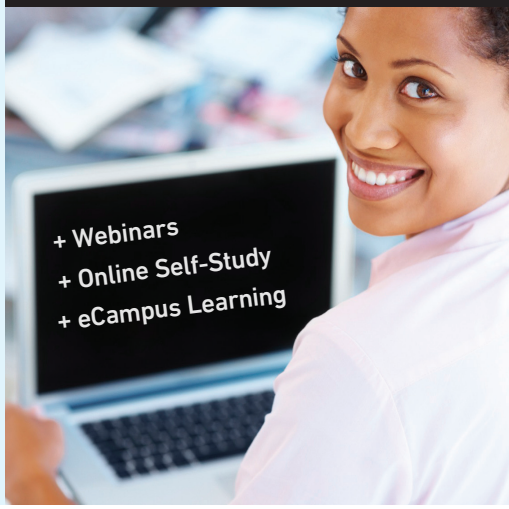
The CAE Master's Program
June 12-14, 2017
Omni Chicago Hotel
Chicago, IL
www.misti.com/OAM590

SuperStrategies 2017
September 11-13, 2017
Planet Hollywood Resort & Casino
Las Vegas, NV

TABLE OF CONTENTS

E-LEARNING COURSES

Can't get away from the office? MISTI has online training options for you. See page 10-11 for details.



2016-2017 SEMINAR SCHEDULE

AH Anaheim
AT Atlanta
BO Boston
CH Chicago
CM Costa Mesa, CA
DA Dallas

Pg. #	Course Code		SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER	JANUARY
INTERNAL/OPERATIONAL AUDIT - GENERAL							
12	OAG101	Fundamentals of Internal Auditing	SF 12-14 **CH 19-21**	**NY 17-19**	BO 2-4 AH 14-16	**OR 12-14**	PH 23-25
13	OAG201	Advanced Auditing for In-Charge Auditors	**CH 19-21**	**NY 17-19**	LV 2-4	**OR 12-14**	LV 23-25
14	OAG115	Organizational Development and Consulting for Auditors			CH 14-16		
14	OAG116	Communication and Change Implementation Skills for Auditors	BO 12-14				
15	OAG111	Effective Business Writing for Auditors		**NY 20-21**			
15	OAG120	Interviewing Techniques for Effective Audits	**CH 22-23**				
16	OAG211	Project Management for Auditors		**NY 20-21**			
16	OAG223	Root Cause Analysis		BO 6-7			
17	OAP301	Internal Audit School	SF 26-29	CH 24-27		LV 5-8	
17	OAP231	Auditing the Manufacturing Process					
18	OAP234	Auditing Supply Chain Management			DA 7-9		
18	OAP311	Process Flow Auditing		DC 17-19			
19	OAP315	Lean Six Sigma Skills for Auditors					
19	OAP362	How to Perform and Benefit from a Peer Review NEW!		OR 3-4			
20	OAP320	Six Sigma White Belt for Auditors NEW!					
20	OAP321	Six Sigma Yellow Belt for Auditors NEW!		OR 3-5			
21	OAP420	Six Sigma Green Belt for Auditors NEW!				OR 12-16	
21	OAG260	Auditing Networks for Non-IT Auditors			SF 2-3		
INTERNAL/OPERATIONAL AUDIT - MANAGEMENT							
22	OAM510	The Audit Leadership Institute					
23	OAM590	The CAE Master's Program					
24	OAG520	Advanced Internal Audit Masterclass NEW!	NY 26-28				
24	OAM302	Audit Manager's Guide to IT Risks			SF 2-3		
25	OAM401	Managing the Internal Audit Department				SF 5-7	
25	OAM425	High-Impact Skills for Developing and Leading Your Audit Team			NY 30-12/2		
FRAUD AUDITING & DATA ANALYTICS							
26	OAF201	Fraud Audit School			SF 14-17		
27	OAF411	Advanced Fraud Audit School					
27	OAF301	Fraud Testing: Integrating Fraud Detection into Your Audit Program		**NY 17-19**			
28	OAF315	Fraud Data Analytics	CH 26-28			**OR 12-14**	
28	OAP215	Data Mining for Auditors				**OR 12-14**	
29	OAF211	The Auditor's Guide to Money Laundering			NY 3-4		
29	OAF340	Bribery and Corruption: FCPA and UK Bribery Act Compliance				**OR 15-16**	
30	OAF403	Fraud in Financial Accounts and Statements NEW!		**NY 20-21**			
30	ITF221	Combating Computer Fraud NEW!			NY 7-9		
31	ITP250	Successful Audit Data Analytics HANDS-ON		NY 24-26	DC 29-12/1	SF 5-7	MI 30-2/1
RISK-BASED AUDITING							
32	OAR201	Risk School	**CH 19-22**	SD 11-14			
33	OAR250	Building a Continuous Risk Assessment Model					
33	OAR321	Using Risk Assessment to Build Individual Audit Programs			LV 14-16		
34	OAR330	Auditing Strategic Risks					
34	OAR341	Auditing the Enterprise Risk Management Process		OR 5-7		BO 5-7	
35	OAR510	Risk Management Masterclass NEW!			NY 14-16		
FINANCIAL INSTITUTION & INVESTMENTS AUDITING							
36	OAP385	Bank Internal Audit School			NY 7-10		
37	OAP380	Auditing Asset Management NEW!		CH 5-7			
37	OAP382	Auditing Debt Collection NEW!		CH 3-4			

DC Washington, DC
DV Denver
HO Houston
LV Las Vegas
MI Miami
NY New York
OR Orlando
PH Phoenix
SD San Diego
SF San Francisco
TP Tampa

Bold Dates Indicate Training Weeks

FEBRUARY	MARCH	APRIL	MAY	JUNE	JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER
SF 6-8	**LV 13-15**	HO 3-5 **BO 24-26**	**DC 15-17**	**NY 12-14**	CH 10-12	**DC 7-9** **AH 21-23**	DC 6-8	SD 2-4 **NY 23-25**	AT 6-8 LV 27-29	**OR 4-6**
SF 6-8	MI 6-8	**BO 24-26**	CH 1-3	**NY 12-14**	DC 31-8/2	**AH 21-23**	BO 6-8	**NY 23-25**	SF 6-8	OR 11-13
			CH 22-24	**SD 5-7**		DC 2-4	BO 6-8			SF 18-20
	SF 6-8					NY 28-30		CH 2-4		
		BO 27-28	**DC 18-19**				**CH 28-29**			
	SF 9-10				**BO 20-21**			OR 19-20		
				BO 15-16		**AH 24-25**		**NY 26-27**		
SF 9-10		**BO 27-28**				**AH 24-25**				**OR 7-8**
TP 13-16	LV 20-23		**DC 15-18**	**SD 5-8**	**BO 17-20**	**DC 7-10**	**CH 25-28**			SF 18-21
AH 22-24					CH 12-14			**NY 23-25**		
	NY 6-8						SF 18-20		BO 27-29	
		CH 3-5				DC 14-16			AH 27-29	
	NY 9-10			**SD 8-9**			SF 21-22			
	OR 9-10			**NY 15-16**				SF 16-17		
OR 13-15					BO 24-26			SF 16-18		
	OR 6-8					BO 14-16			SF 13-15	
			OR 1-5				BO 18-22			SF 11-15
SF 9-10			**DC 18-19**				**CH 28-29**			
						BO				
				CH 12-14						
		BO 3-5				DC 2-4			SF 13-15	
	CH 9-10					**DC 10-11**		SF 2-3		
	OR 13-15			**SD 5-7**			**CH 25-27**			
LV 27-3/1			BO 22-24					OR 16-18		
			DC 15-18	**NY 12-15**		**AH 21-24**		**NY 23-26**		
		NY 25-28			CH 10-13			BO 10-13		
			NY 22-24		**BO 17-19**			SD 2-4		**OR 4-6**
				SD 5-7		NY 14-16	**CH 25-27**			OR 18-20
	SD 20-22					NY 28-30		OR 9-11		
	SF 9-10			**NY 15-16**					DC 2-3	
				SD 8-9						**OR 7-8**
			NY 1-2		BO 24-25			SD 5-6		
					BO 17-19					
	LV 20-22		BO 8-10		DC 24-26		CH 18-20	NY 10-12	SF 13-15 OR 29-12/1	
PH 27-3/2		**BO 24-27**		AH 19-22			CH 18-21		OR 13-16	
SF 9-10				**NY 15-16**						OR 7-8
	LV 13-15			**NY 12-14**						OR 4-6
		NY 19-21			**BO 17-19**		CH 11-13			
SF 6-8			OR 8-10			**DC 7-9**			CH 6-8	
			NY 1-3					CH 16-18		
	NY 20-23			CH 19-22	BO 31-8/3				SF 13-16	
		BO 3-5			DC 24-26			SF 30-11/1		
		BO 6-7			DC 27-28				SF 2-3	

SEMINAR SCHEDULE

2016-2017 SEMINAR SCHEDULE

AH Anaheim
AT Atlanta
BO Boston
CH Chicago
CM Costa Mesa, CA
DA Dallas

Pg. #	Course Code		SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER	JANUARY
FINANCIAL INSTITUTION & INVESTMENTS AUDITING (CONTINUED)							
38	OAP285	Understanding and Auditing Investments and Derivatives			CH 2-4		
38	OAP381	Community Banking Governance and Assurance Practices					
39	OAR385	Auditing Basel III and the ICAAP/RRP				NY 7-9	
39	OAP384	Auditing the Credit Department				NY 5-6	
GOVERNANCE & COMPLIANCE							
40	OAP241	COSO 2013 Internal Control Integrated Framework	CH 22-23			OR 15-16	
40	OAP352	Governance, Risk and Compliance		NY 17-19			
41	ITP241	COBIT® 5: Integrating the COBIT into Your IT Audit Process					
41	ITP262	Testing IT General Computer Controls for Sarbanes-Oxley					SF 30-31
IT AUDITING							
42	ITG101	IT Auditing and Controls	CH 19-21	DA 4-6	SF 10/31-2	MI 5-7	
43	ITG103	Auditing Business Application Systems			SF 3-4		
44	ITG121	IT Audit School	SD 12-15	NY 17-20	LV 7-10	OR 12-15	
45	ITG241	Intermediate IT Audit School	SF 26-29	NY 17-20	LV 14-17	OR 12-15	
46	ITG341	Advanced IT Audit School	CH 19-22		NY 7-10		
46	ITG213	Auditing Agile and Scrum Development Projects NEW!					
47	ITG212	Auditing Application Systems Development	CH 19-21				
47	ITG231	Preparing for the CISA® Examination					
48	ITP361	A Risk-Based Guide to IT Infrastructure Controls		DC 4-6			
48	ITP265	Integrating Emerging Technology Threats in Your Annual Risk Assessment		MI 24-26			
INFORMATION SECURITY							
49	ISG101	Introduction to Information Security				OR 12-14	
49	ISG103	Practical Security Assessments HANDS-ON NEW!	OR 26-27			SF 5-6	
50	ISG120	Tools to Identify and Mitigate Security and Privacy NEW!			SF 28-30		
50	ISG231	Data Privacy: Protecting Your Organization, Customers and Employees					
51	ASG203	Network Security Essentials		NY 17-19		OR 12-14	
51	ISG291	Information Security Boot Camp	CH 19-23			AH 5-9	
52	ISG320	Introduction to Incident Response			NY 9-10		
52	ISG301	Managing Mobile Device Security HANDS-ON					
53	ISG391	Information Security Academy NEW!					
53	ISM230	Building an Effective Information Security Program Using Security Frameworks NEW!					
54	ISG240	Business Continuity Planning and Disaster Recovery Assurance Practices			BO 14-15		
AUDIT & SECURITY - NETWORKS & ENTERPRISE APPLICATIONS							
55	ASE241	Audit and Security of SAP® ERP HANDS-ON		DV 4-7	DC 14-17		PH 23-26
56	ASE441	Advanced SAP® ERP Audit and Security HANDS-ON	NY 14-16				
56	ASE351	Auditing and Securing Oracle® Databases	CH 12-15				
57	ASE355	Auditing Oracle's® E-Business Suite				SF 12-14	
57	ASG231	Securing and Auditing Your Network Infrastructure HANDS-ON		NY 31-11/4			
58	ASG232	Securing and Auditing Your Application Software Infrastructure HANDS-ON					
58	ASN304	Securing and Auditing Virtualized Environments		NY 24-28			
59	ASN305	Audit and Security for Cloud-Based Services	NY 26-27			CH 8-9	
60	ASN311	Auditing Encryption		BO 12-14			
61	ASO402	Securing and Auditing Windows Active Directory Domains HANDS-ON			NY 1-4		
ACL CERTIFIED COURSES							
63	ACL101	ACL® 101 Foundations HANDS-ON NEW!	CM 12-14 DA 26-28	BO 11-13 CH 24-26	DC 14-16	SF 5-7	HO 23-25
64	ACL201	ACL® 201 Applications HANDS-ON NEW!	CM 15-16 DA 29-30	CH 27-28		SF 8-9	HO 26-27
64	ACL303	ACL® 303 Scripting HANDS-ON NEW!	DA 26-28	CH 24-26	DC 14-16		

DC Washington, DC
DV Denver
HO Houston
LV Las Vegas
MI Miami
NY New York
OR Orlando
PH Phoenix
SD San Diego
SF San Francisco
TP Tampa
Bold Dates Indicate Training Weeks

FEBRUARY	MARCH	APRIL	MAY	JUNE	JULY	AUGUST	SEPTEMBER	OCTOBER	NOVEMBER	DECEMBER
	LV 13-15		NY 8-10			CH 28-30				SF 4-6
SF 6-8				NY 7-9				BO 9-11		
			NY 8-10				**CH 25-27**			
	LV 16-17		NY 11-12				**CH 28-29**			
SF 9-10			**DC 18-19**							**OR 7-8**
	NY 13-15		AH 22-24					CH 16-18		
			SF 8-10					**NY 23-25**		
			BO 11-12				CH 14-15			
SF 6-8	DV 27-29	**BO 24-26**	CH 1-3	**SD 5-7**	**BO 17-19**	**DC 7-9**	OR 18-20	CH 11-13	AH 6-8	**OR 4-6**
			CH 4-5				OR 21-22			**OR 7-8**
AT 27-3/2	**LV 13-16**	CH 18-21	**DC 15-18**	**NY 12-15**	DV 24-27	**AH 21-24**	**CH 25-28**	**NY 23-26**	BO 13-16	SD 18-21
TP 13-16	**LV 13-16**	AT 18-21	**DC 15-18**	**NY 12-15**	CH 10-13	**AH 21-24**	DV 11-14	**NY 23-26**	CH 14-17	OR 4-7
		BO 24-27		**SD 5-8**		**DC 7-10**			OR 27-30	
		BO 27-28			**BO 20-21**					
SF 6-8			**DC 15-17**					**CH 16-18**		
			CH 1-4			BO 14-17				
		BO 24-26				**DC 7-9**		CH 9-11		
	LV 13-15		NY 8-10				SF 6-8		OR 8-10	
	LV 13-15			**SD 5-7**		**DC 7-9**				**OR 4-6**
		OR 27-28							SF 16-17	
SF 8-10				**NY 12-14**	**BO 17-19**					**OR 4-6**
	LV 20-22	**BO 24-26**				NY 21-23				
SF 6-8			**DC 15-17**		**BO 17-19**	**AH 21-23**		**NY 23-25**		
		BO 3-7		**NY 12-16**			**CH 25-29**		SF 27-12/1	
	LV 16-17					**DC 10-11**		**NY 26-27**		
		OR 24-26					SF 11-13			
SF 27-3/2			NY 1-4			CH 21-24				
	SF 9-10			BO 8-9				CH 19-20		
	OR 23-24			DC 22-23					BO 2-3	
	NY 28-31		OR 8-11			CH 14-17		DC 2-5		SF 18-21
		SF 19-21					NY 19-21			
			CH 8-11						OR 27-30	
		NY 24-26						SF 9-11		
	SF 20-24			DC 26-30			AH 25-29	NY 30-11/3		
SF 6-10			DC 1-5			AH 21-25				AT 18-22
			BO 1-5			CH 14-18			SF 27-12/1	
		BO 27-28		**SD 8-9**		**DC 10-11**		CH 16-17		
	LV 13-15			**NY 12-14**			**CH 25-27**			
	AT 27-30		**DC 15-18**			AH 1-4		**NY 23-26**		
NY 13-15	AT 6-8	CH 3-5 DA 24-26	SF 8-10 DC 22-24	NY 19-21						
	AT 9-10		SF 11-12	NY 22-23	*More ACL101, 201 & 303 dates coming soon! Visit www.misti.com/acl					
NY 13-15		DA 24-26								

SEMINAR SCHEDULE

IN-HOUSE TRAINING

Customizable, Timely and Cost-Effective

Why should you schedule in-house training for your staff?

- In-house training develops skills that increase your team's productivity and the quality of their work product.
- Well trained staff are more engaged, with higher morale and initiative, which helps you retain your people.
- Timely training is imperative if you're going to mitigate risk in the face of ever-changing legislative and market challenges.

What are the advantages of choosing the in-house training option?

- **Save time and money:** If six 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. 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 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 team members:** 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 and learns the same methods. 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!

For more information, contact:
Mimi Hatch, at (508) 532-3623 or mhatch@misti.com.

Bring a MISTI Seminar to your professional association chapter

- In-House seminars are 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, information technology audit, information security management, control and governance, assurance and risk management.

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

"The training was well-tailored to the needs of internal and external auditors. I will definitely use what I learned in my daily job."

IT Audit Manager, Brown Brothers Harriman

"Should be a 'must have' course for any person entering into a security job."

Senior Security Engineer, Edward Jones

MISTI CERTIFICATE PROGRAMS

Skills, Confidence and Credibility

MISTI has developed tailored certificate curricula to aid IT Audit, Internal Audit and Information Security professionals gain the vital skills, confidence and, most importantly, the credibility they need to succeed in their specialized roles and respective disciplines. MISTI Certificates are an objective, measurable way to demonstrate professional competence and validate your professional standing.

How Certificate Programs Work

Each certificate program below consists of four courses. In each category, you must attend at least one of the Required Seminars listed plus three of the Elective Seminars within the categories listed. Required Seminar choices can also count toward one of your Elective Seminars. You will have a 30 month time period in which to complete all four courses.*

Benefits of the MISTI Certificate Programs – you will receive:

- A framed certificate of completion for the program fulfilled
- 15% off the total cost of all four seminars*
- 10% off all instructor-led programs for one year after completion of certificate program*
- 10% off all conferences offered for one year after completion of certificate program

Internal Audit Certificate

Required Seminars *(choose one):*

- Fundamentals of Internal Auditing (OAG101)
- Internal Audit School (OAP301)
- Managing the Internal Audit Department (OAM401)

PLUS three electives in any of these categories:

- Internal/Operational Audit – General
- Internal/Operational Audit – Management
- Fraud Auditing and Data Analytics
- Risk-Based Auditing
- Financial Institution and Investments Auditing
- Governance and Compliance

Fraud and Data Analytics Certificate

Required Seminars *(choose one):*

- Fraud Audit School (OAF201)
- Fraud Data Analytics (OAF315)
- Successful Audit Data Analytics (ITP250)

PLUS three electives in this category:

- Fraud Auditing and Data Analytics

Risk and Compliance Certificate

Required Seminars *(choose one):*

- Risk School (OAR201)
- Auditing the Enterprise Risk Management Process (OAR341)
- Governance, Risk and Compliance (OAP352)

PLUS three electives in any of these categories:

- Risk-Based Auditing
- Governance and Compliance

IT Audit Certificate

Required Seminars *(choose one):*

- IT Auditing and Controls (ITG101)
- IT Audit School (ITG121)
- Intermediate IT Audit School (ITG241)

PLUS three electives in any of these categories:

- IT Auditing
- Audit and Security – Networks and Enterprise Applications

Information Security Certificate

Required Seminars *(choose one):*

- Fundamentals of Information Security and Controls (ISG101)
- Network Security Essentials (ASG203)
- Information Security Boot Camp (ISG291)

PLUS three electives in any of these categories:

- Information Security
- Audit and Security – Networks and Enterprise Applications

***Certificate Program Details:**

- *Your 15% discount is applied to the fourth seminar completed in the program*
- *Discounts listed above do not apply to in-house, online self-study, webinar or eCampus courses attended*
- *In-House, online self-study, webinar and eCampus courses **cannot** count towards completing your certificate program*
- *Seminars used to fulfill requirements of one program **cannot** be used to fulfill the requirements of a different program*
- *Certificate Program discounts **cannot** be combined with any other MISTI discounts*
- *If you have taken a seminar that is no longer listed please contact our Customer Service department at (508) 879-7999 ext. 501*

MISTI Webinars

MISTI's offering of live webinars is the perfect solution for the busy professional looking for expert training. Webinars are a growing source of NASBA certified CPE credits for our clients. These interactive, live webinars are ideal for internal auditors, IT auditors and information security professionals who want to stay abreast of industry trends and bring immediate and relevant value to their organizations. MISTI recruits industry leaders to teach these information-packed live webinars. Our instructors bring their real-world experience to attendees, offering them practical solutions to everyday challenges.

Some of our popular webinars include:

- Risk-Based Auditing of Agile and Scrum RAD Projects
- Information Security Essentials for Non IT Auditors
- Controlling Audit Projects: Tip and Tricks
- Leading Effective Exit Meetings
- Combating Computer Fraud
- IT Risk-Based Audit Planning Strategies
- Auditing and Preventing Fraud in Procurement
- Introduction to Networks
- Social Engineering and Physical Threat Assessments

Benefits of MISTI's Live Webinars:

- Earn NASBA certified CPE Credits
- No travel expenses or planning
- Affordable tuition fees
- Maximize learning in less time
- Advantage of learning from your office or home
- Knowledge to put into play immediately
- Access to our seasoned, experienced instructors

MISTI often adds new webinars to its curriculum and is regularly scheduling live webinar dates. For a listing of our currently scheduled webinars, please visit: **www.misti.com/LIVEWebinars.**

Can't Attend the Scheduled Live Session?

We have that covered! We know a lot of working professionals cannot always make the scheduled times of our live webinars. For this reason, MISTI records most webinars so they can be purchased and viewed on demand, at your own convenience! These recordings are available to you for seven calendar days after they are purchased, giving you ample time to learn. For a listing of our recorded webinars, please visit: **www.misti.com/RecordedWebinars.**

"My main goal was to find ways to get our auditees to fill out the post audit survey and I heard several things during the webinar I can do to increase the response rates. I'm so glad I attended!"

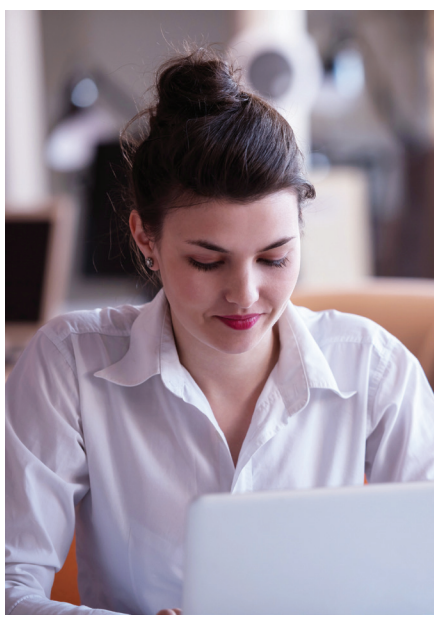
From Using Surveys in Internal Audits with Dr. Hernan Murdock, CIA, CRMA

"Very good. Gave really great examples of how the tools can be used both personally and professionally. Could tell the instructor had a passion for the topic."

From Audit Lessons from Recent Security Breaches with Fred C. Roth, CISA

"This was very helpful. The webinar was clear and I appreciated all the examples given. It was very well done and gave me the knowledge I need as a new auditor."

From Developing Essential Fieldwork Skills with Bill Woodington, CPA, CIA



MISTI Online Self-Study

MISTI Online Self-Study makes it possible to benefit from our most popular seminar topics, learn at your own pace, earn CPEs and save on travel costs. You are able to log on to these interactive courses and learn through extensive PowerPoint presentations, including exams, from your home or office. As each module is successfully passed (a minimum 60% score on each exam) your progress is updated.

Online Self-Study Courses

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 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

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

Preparing for the CISA® Exam: This self-study focuses exclusively on the essential areas covered in the CISA exam. Participants will cover the content areas needed to know for the exam, including IS audit process, IT governance, systems and infrastructure life cycle management, IT service delivery/support, information asset protection, business continuity and disaster recovery.
31 CPEs - Tuition: $1995

Note: Online courses vary from catalog descriptions. For full Online Self-Study course descriptions and more information, please visit: ***www.misti.com/Self-Study****.*

MISTI eCampus

MISTI is excited to offer a new web-based option that provides more online training and education options for professionals. This offering is provided by SmartPros and offers certified CPE courses in accounting, auditing, finance, management and other areas. All courses are online, self-paced courses that you access at your convenience. As each course is successfully passed each individual's course journal is updated. The credits earned in these accounting courses can be applied towards a CPA, CMA and CFM certification.

Subscription Programs Offered

SmartPros Advantage:
SmartPros Advantage is an annual subscription of hundreds of multi-media and text driven "skills-based" courses for one low price. Choose from categories including accounting and auditing, financial planning, consulting, management, computer applications, taxation and more! With this subscription you get unlimited access to the entire catalog. All courses qualify for CPE credit under NASBA QAS certification.
MISTI Subscription Price $339 +tax (regular $464).

Financial Management Network (FMN) Online & DVD:
FMN produces 48 new courses, 4 every month and has more than 72 archived courses. An annual subscription includes "fast track" outlines, transcripts, quizzes and the ability to track credits and print completion certificates. All courses qualify for CPE credit under NASBA QAS certification. FMN features top industry experts discussing topics and issues at the forefront of today's finance and accounting professionals.
MISTI Subscription Price $339 +tax (regular $464).

To browse these subscription based options in more detail, please visit: **www.misti.com/eCampus.**

Fundamentals of Internal Auditing

AVAILABLE ONLINE

Learning the Building Blocks for Performing Effective Audits

Seminar Focus and Features

In this three-day seminar you will learn the concepts of traditional and operational auditing and gain proven tools and techniques for performing effective audits. You will get a solid background in the basics of documenting and evaluating internal control/fieldwork techniques. 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 focus on and put into practice the communication skills associated with internal auditing: conferencing with customers, writing audit findings and selling audit recommendations.

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

TOP 10 IN-HOUSE

Who Should Attend

Financial, Operational and Information Technology Auditors with less than two years of audit experience

BONUS

Standards for the Professional Practice, invaluable sample documents for use as models for your drafts; the COSO overview; and complete text of the Sarbanes-Oxley Act

What You Will Learn

1. **Internal Auditing**
   - IA department sample charter
   - the role of the IA department
   - the *Standards*
   - leading-edge trends in IA
   - what makes an effective IA department
   - differences between an internal auditor/external auditor
   - events that have helped create growth in IA
   - the Foreign Corrupt Practices Act (FCPA)
   - COSO IC-IF
   - Federal Sentencing Guidelines
   - Sarbanes-Oxley
   - fraudulent financial reporting
   - IA department sample statement of purpose
2. **Contemporary Internal Auditing**
   - types of internal audits
   - economy, efficiency and effectiveness
   - operational vs. financial auditing
   - overview of IT General Computer Controls (GCCs) and COBIT®
   - steps in the IA process: an overview
3. **Risk Assessment Strategies**
   - selecting the client
   - notifying the client
   - determining risk
   - performance standard for determining risk
   - effects of risk
   - identifying auditable activities
   - risk factors
   - trends in risk assessment
   - risk assessment approaches
4. **Planning and Preliminary Fieldwork**
   - strategies for planning the audit
   - notifying the client
   - the planning memo
   - preliminary and opening meetings
   - the importance of preliminary work
   - strategies for planning effectively
   - planning resources
5. **Documenting Internal Controls**
   - evaluating and documenting the system of internal controls
   - performance standard for controls
   - control points
   - cost/benefit considerations
   - types of controls
   - the control environment
   - methods of documenting internal controls
   - internal control questionnaire
   - flowcharts
6. **Audit Programs**
   - performance standards, scope and developing the audit program
   - the audit program as a guide
   - criteria for audit programs
   - audit objectives/scope/test steps
   - sample audit program
7. **Fieldwork Techniques**
   - performance standards for fieldwork
   - audit evidence
   - handling sensitive evidence
8. **Workpapers**
   - performance standards for recording information and engagement supervision
   - purpose of audit workpapers
   - workpaper techniques/ templates
   - electronic workpapers
   - tick marks
   - quality assurance and improvement program
9. **Audit Findings**
   - performance standards for communicating results and monitoring progress
   - attributes of audit findings
   - selling your audit findings
   - template for audit findings
10. **Audit Reports**
    - fundamentals of audit reports
    - selling your report
    - strategies for issuing timely reports
    - characteristics of effective audit reports
11. **Effective Audit Communications**
    - possible barriers to overcome in the interview
    - diffusing the difficult interview
    - dos and don'ts of effective interviewing
    - strategies for conducting effective closing meetings
12. **Sampling**
    - sampling and its effect on audit testing
    - sampling terminology and methodologies
    - sampling for SOX

SCHEDULE

September 12-14, 2016
San Francisco, CA

September 19-21, 2016
Chicago, IL

October 17-19, 2016
New York, NY

November 2-4, 2016
Boston, MA

November 14-16, 2016
Anaheim, CA

December 12-14, 2016
Orlando, FL

January 23-25, 2017
Phoenix, AZ

February 6-8, 2017
San Francisco, CA

March 13-15, 2017
Las Vegas, NV

April 3-5, 2017
Houston, TX

April 24-26, 2017
Boston, MA

May 15-17, 2017
Washington, DC

June 12-14, 2017
New York, NY

July 10-12, 2017
Chicago, IL

August 7-9, 2017
Washington, DC

August 21-23, 2017
Anaheim, CA

September 6-8, 2017
Washington, DC

October 2-4, 2017
San Diego, CA

October 23-25, 2017
New York, NY

November 6-8, 2017
Atlanta, GA

November 27-29, 2017
Las Vegas, NV

December 4-6, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAG101

Advanced Auditing for In-Charge Auditors

AVAILABLE ONLINE

Developing and Managing Risk-Based Audits That Add Value

Seminar Focus and Features

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

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

TOP 10 IN-HOUSE

Who Should Attend

Financial, Operational, Information Technology and External Auditors with two or more years of audit experience

What You Will Learn

1. **Managing Fieldwork**
   - reasons why internal audit must add more value
   - fieldwork management: in-charge's perspective
   - fieldwork methodology tools
   - fieldwork methodology selection
   - workpaper review
   - samples of evaluations
   - overview of the Professional Standards
2. **Auditing Concepts: The In-Charge's Perspective**
   - responsibilities of the IA department
   - losing credibility
   - operational vs. financial/ compliance auditing
   - essentials of operational auditing
   - the audit triangles
   - questions an audit attempts to answer
3. **The Control Environment: High-Impact Changes**
   - the changing control environment
   - emphasis on key controls
   - soft/hard controls
   - balance risks and controls
   - examples of entity level controls
   - changes since sarbanes-oxley
   - corporate governance
   - blue ribbon committee on corporate audit committees
   - Sarbanes-Oxley overview
   - COSO executive summary
   - the control environment to avoid
4. **Marketing and Selling Internal Audit**
   - key factors in marketing and selling the audit function
5. **Preliminary Fieldwork and Program Development**
   - allocating time
   - impact and benefits of data analytics
   - simple data mining model
   - when to consider data mining
   - areas to consider for a more productive audit
   - the audit program
   - criteria for audit programs
   - group exercise
   - how to manage an audit
6. **Risk Assessment Strategies**
   - what is risk assessment?
   - what the in-charge needs for every audit
   - differentiate enterprise risk and audit risk
   - differentiate inherent risk and residual risk
   - criteria for effective risk assessment
   - best practices for identifying emerging risks earlier
   - risk environment
   - trends in risk assessment
   - four assets of audit departments
   - gross risk and net risk
   - risk matrix
   - the successful risk model
   - audit level risk assessment factors
   - ERM dos and don'ts
7. **Applying Project Management to Internal Audit**
   - project approaches to audit teams
   - key factors to successful audit/ project management
   - the audit/project planning process
   - using project management to effectively plan audits
   - time estimates
   - common workflow planning problems
   - audit/project leader's responsibilities
   - resource management
   - guidelines and examples of good audit/project management
   - time management improvement issues
8. **Fraud Awareness**
   - impact of Sarbanes-Oxley in addressing fraud
   - what is fraud?
   - fraud triangle
   - key findings and conclusions from 2014 ACFE report to the nations
   - what to do when you suspect fraud
   - areas of fraud occurrence
   - indicators of potential fraud
   - most successful techniques for preventing and detecting fraud
   - the hallmarks of an effective compliance program
   - auditing tone at the top
9. **Effective Communications**
   - Professional Standard #2420
   - dos and don'ts of effective meeting management
   - trends in audit report formats
   - executive summary options
   - recommendation options
   - guidelines for issuing more timely reports
   - closing conference strategies currently in practice
10. **High-Profile Case Studies**
    - Sunbeam issues
    - Enron/Andersen
    - Allied Irish Bank
    - Wal-Mart
    - Tyco
    - ImClone/Martha Stewart
    - WorldCom
    - Healthsouth
    - Madoff
    - others
11. **Improving Productivity**
    - measuring internal audit productivity
    - planning/fieldwork
    - writing/wrap up
    - potential productivity decreases
    - improving productivity of audit management
    - increasing auditor productivity
12. **Best Practices in Internal Audit**

SCHEDULE

September 19-21, 2016
Chicago, IL

October 17-19, 2016
New York, NY

November 2-4, 2016
Las Vegas, NV

December 12-14, 2016
Orlando, FL

January 23-25, 2017
Las Vegas, NV

February 6-8, 2017
San Francisco, CA

March 6-8, 2017
Miami, FL

April 24-26, 2017
Boston, MA

May 1-3, 2017
Chicago, IL

June 12-14, 2017
New York, NY

July 31-August 2, 2017
Washington, DC

August 21-23, 2017
Anaheim, CA

September 6-8, 2017
Boston, MA

October 23-25, 2017
New York, NY

November 6-8, 2017
San Francisco, CA

December 11-13, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAG201

OAG115

Organizational Development and Consulting for Auditors

Add More Value to Your Organization through Skill Building and Career Enhancement

Seminar Focus and Features

This three-day seminar is designed to help auditors expand their horizons by gaining an understanding of the field of Organization Development (OD). The course will cover front-line research and established practices from leading organizations that provide essential insights and useful tools for managing OD challenges.

You will discover creative methods to establish relationships and collaborate with executives and leaders at all levels, ascertain and evaluate corporate needs, unravel serious strategic challenges, apply OD solutions to accomplish business objectives and produce a balanced change management process. You will gain an understanding of different models for strategy and OD execution that incorporates a full range of proven approaches and emerging concepts to align OD initiatives with corporate objectives.

Auditors will learn how OD utilizes behavioral science to assist corporate leadership during the change management process and generate impactful solutions that enhance corporate strategy, culture and business execution.

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

Who Should Attend

Internal and External Audit staff all levels; Business Advisory Professionals; Training and Development Professionals; Organization Development Professionals

What You Will Learn

1. **Introduction to the Field of OD**
2. **Exploring OD Roles, Tools, Relationships, Interviews, Data**
3. **Evaluating Change and Project Readiness**
4. **Strategy – Development and Execution**
5. **Examining the Different Aspects and Components of the Organization**
6. **Organizational Alignment to Enhance Synergy**
7. **Reviewing OD and Strategic Models for Success**
8. **Reviewing the "Good to Great" Model from an OD Perspective**
9. **Organizational Behavior**
10. **Utilizing OD Models in Action**
11. **Compare and Contrast OD and IA**

SCHEDULE

November 14-16, 2016
Chicago, IL

May 22-24, 2017
Chicago, IL

June 5-7, 2017
San Diego, CA

August 2-4, 2017
Washington, DC

September 6-8, 2017
Boston, MA

December 18-20, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAG115

OAG116

Communication and Change Implementation Skills for Auditors

Proven Communication Techniques for Building Strong Client Relationships and Gaining Acceptance of Your Findings

Seminar Focus and Features

In this practical and interactive three-day seminar you will learn targeted communication strategies and effective influencing tactics for interacting with different work styles. You will learn and apply proven change implementation skills that use a tested equation that will raise your professional profile while increasing Audit's value to the organization. You will master tools and techniques you can use to enhance your communication and change implementation skills, including learning how to better work across distance and cultures with global audit teams and auditees. You will cover the steps to take to build good client relationships and tackle such thorny issues as dealing with disagreement before it gets out of control, understanding cultural differences, delivering bad news, partnering with your clients to help them successfully implement audit findings and more.

In addition, if you are currently wrestling with a specific communication challenge, we urge you to bring it with you so you can apply your learnings to your real-world situation. Activities throughout the seminar will let you put theory into practice. You will leave this intensive seminar with the tools you need to boost your interpersonal skills and your ability to influence others to optimize your value as an Internal Auditor.

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

Who Should Attend

Audit Managers and Supervisors; Internal and External Auditors; staff who have responsibility for presenting audit findings; and those who want to improve their influencing and communication skills

What You Will Learn

1. **How Your Work Style Impacts Communications and Engagements**
2. **Communicating/Working in a Multicultural and/or Virtual Work Setting**
3. **Building Your Change Implementation Skills to Help Gain Acceptance of Your Findings**
4. **Building Your Change Implementation Engagement and Communication Skills**
5. **Influencing and Listening Styles**
6. **Diffusing Difficult Situations: How to Take Corrective Measures When Things Go Wrong**

SCHEDULE

September 12-14, 2016
Boston, MA

March 6-8, 2017
San Francisco, CA

August 28-30, 2017
New York, NY

October 2-4, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAG116

OAG111

Effective Business Writing for Auditors

Writing Skills That Get Results

Seminar Focus and Features

Effective writing skills are a core component of creating a powerful audit report. This seminar covers general writing topics such as the building blocks of writing to achieve results, determining audience and purpose, mindmapping, transparent structure, cutting the clutter, making sentences make sense, subject/verb agreement, parallel construction, efficient editing and active/passive voice. It will also cover topics specific to audit reports by evaluating audit report writing samples, creating an audit Issue and Recommendation (I&R), agreement with antecedents, proofreading your report and effective emails. You will critique examples from actual audit reports to improve your writing skills.

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

BONUS
Attendees will receive *The Gregg Reference Manual.*

Who Should Attend

Audit Managers, Supervisors and staff who have overall or partial responsibility for presenting audit findings; those who need to improve report writing or editing skills

What You Will Learn

1. **The Building Blocks of Writing to Achieve Results**
2. **Writing Basics: Determining Audience and Purpose**
3. **Mindmapping: Organizing for Results**
4. **Transparent Structure: Making Reading Easy**
5. **Cutting the Clutter**
6. **Making Sentences Make Sense**
7. **Writing Findings and Recommendations**
8. **Fixing the Micro**
9. **Editing**
10. **Proofreading**

SCHEDULE

October 20-21, 2016
New York, NY

April 27-28, 2017
Boston, MA

May 18-19, 2017
Washington, DC

September 28-29, 2017
Chicago, IL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAG111

OAG120

Interviewing Techniques for Effective Audits

Conducting Interviews That Improve the Audit Process

Seminar Focus and Features

The interview is a tool at the center of each audit. It is a method for gathering facts, gaining understanding of systems and processes, clarifying information and insights and uncovering fraud and deception. Yet interviewing can be one of the more challenging aspects of the internal audit process – good interviews do not just happen. They are the result of careful planning, thorough preparation and deliberate use of specific communication skills and techniques.

In this two-day session, you will learn how to encourage people to share information, manage conversational flow, pay attention and respond to behavioral clues, capture details and insights provided by the interviewee and incorporate interview results into an overall audit approach. We will explore and practice interview techniques that will allow you to more effectively obtain the truth, detect lies and deception and gain valuable knowledge throughout the audit process. This highly interactive class includes lecture, class discussion, small group activities and role-playing.

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

Who Should Attend

Internal Auditors, IT Auditors, Senior and In-Charge Auditors, Audit Managers, Team Leaders and Directors

What You Will Learn

1. **Interviewing in the Context of Internal Auditing**
   - interviewing as a skill
   - types of audit evidence
2. **Planning and Preparation**
   - establishing your objectives
   - roles and responsibilities
   - conversational styles
   - verbal and non-verbal dimensions
   - documenting answers
3. **Preparing and Managing the Interviewee**
   - introductions and rapport
   - laying a foundation for understanding and trust
4. **Executing the Interview Itself**
   - asking your planned questions
   - improvising follow-up questions
   - listening to what is said and what is not said
   - observing behavioral clues
5. **Documenting the Interview**
   - making time to document
   - independent vs. collaborative
   - sharing notes with interviewees
6. **Follow-up to Interviews**
   - round two interviewing
   - interviewing other parties
   - designing audit testing to corroborate information

SCHEDULE

September 22-23, 2016
Chicago, IL

March 9-10, 2017
San Francisco, CA

July 20-21, 2017
Boston, MA

October 19-20, 2017
Orlando, FL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAG120

OAG211

Project Management for Auditors

Improving Audit Productivity with Project Management

Seminar Focus and Features

In two intensive days, attendees will learn the basics of project management, including how to achieve improved cost control, resource utilization and timelier audit conclusions. Attendees will participate in hands-on exercises that teach how to apply these techniques to increasing productivity in the internal audit process. Using audit-specific examples, you will learn project planning, scheduling, control and decision support concepts and methodologies - the basics of project management. At the conclusion of the seminar, you will have gained the skills to better initiate, plan, execute, monitor and control, and close your audit, all while decreasing the time and costs required to perform the audit and increasing audit efficiency and quality.

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operational, Information Technology and External Auditors with two or more years of audit experience

What You Will Learn

1. **Project Management and Audit**
   - project management's relevance to internal audit
   - expanding audit project leaders' core competencies
2. **Cornerstones of Project Management**
   - nine knowledge areas of project management
   - mapping, scheduling and controlling the project
   - allocating resources
   - identifying problems early in the process
3. **Applying Project Management Strategies to IA**
   - using project management to plan audits
   - time estimates
   - common workflow planning problems
   - audit/project leader's responsibilities
   - resource management
   - guidelines/examples of good audit/project management
   - improving time management
4. **Applying Project Management to the Audit Process**
   - maximizing your investment in planning and minimizing your investment in fieldwork
   - writing/issuing meaningful reports promptly
5. **Practice Case**
6. **The Successful Project Manager**
7. **Meeting Today's Audit Challenges with Project Management Techniques**
8. **50 Project Management Tips for Improving Audit Productivity**

SCHEDULE

October 20-21, 2016
New York, NY

June 15-16, 2017
Boston, MA

August 24-25, 2017
Anaheim, CA

October 26-27, 2017
New York, NY

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAG211

OAG223

Root Cause Analysis for Internal Auditors

Practical Strategies for Motivating Your Audit Team to Achieve Value-Added Results

Seminar Focus and Features

In this seminar, participants will learn to apply the structured process of Root Cause Analysis (RCA) to their audit practices. The course provides in-depth techniques and tools that will help attendees identify a range of potential root causes for problem areas, select the most likely root cause, investigate at the point of the problem and determine and prioritize potential solutions. Participants will discover the risks and opportunities at each stage of RCA and develop advanced skills to improve communication with all stakeholders.

The purpose of an RCA is to uncover what happened, why it happened and determine what changes need to be made. Once necessary changes have been identified, the recommended resulting actions should be tailored to the environment, resources and people who have to carry out the changes. The techniques covered in this seminar will allow an internal auditor to better understand and convey to management why systems, processes or functional areas are not operating as intended or designed.

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

Internal Auditors motivated to resolve persistent problems

What You Will Learn

1. **Understanding Roadblocks and Consequences of Ineffective Problem-Solving**
   - having limited perspective
   - focusing too closely on rules or behaviors
   - separating and combining different types of thinking
2. **Analyzing Problems Thoroughly**
   - tools and filters for priority setting
   - developing clear and complete problem statements
3. **Gathering and Managing Data**
   - population or sample?
   - surveys, interviews and observations
4. **Pinpointing Cause and Effect**
   - five whys
   - fishbone diagram
   - mind maps
5. **Identifying and Recommending Solutions**
   - CATWOE
   - force field analysis
6. **Organizational Issues**
   - biases, structures and roles for and against RCA
   - understanding resistance to change

SCHEDULE

October 6-7, 2016
Boston, MA

February 9-10, 2017
San Francisco, CA

April 27-28, 2017
Boston, MA

August 24-25, 2017
Anaheim, CA

December 7-8, 2017
Orlando, FL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAG223

OAP301

Internal Audit School

Acquiring the Essential Operational Auditing Skills

Seminar Focus and Features

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

You will explore the objectives of major business operation areas and learn how to identify the key risks threatening them. You will find out how to make your audits more efficient and effective and how to use data analytics to gain an in-depth understanding of business processes. You will cover such critical areas as the impact of SOX, ERM and GRC on the organization, uncovering fraud schemes that threaten business operations and the role of IA in helping management build strong risk management and strategic planning processes. You will learn 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. **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 IT**
8. **Auditing Management and Corporate Governance**
9. **The Future of Operational Auditing**

SCHEDULE

September 26-29, 2016
San Francisco, CA

October 24-27, 2016
Chicago, IL

December 5-8, 2016
Las Vegas, NV

February 13-16, 2017
Tampa, FL

March 20-23, 2017
Las Vegas, NV

May 15-18, 2017
Washington, DC

June 5-8, 2017
San Diego, CA

July 17-20, 2017
Boston, MA

August 7-10, 2017
Washington, DC

September 25-28, 2017
Chicago, IL

December 18-21, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/OAP301

OAP231

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. Seminar 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

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Internal Audit Directors, Managers and Staff; IT Auditors; and External Auditors in manufacturing organizations

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

February 22-24, 2017
Anaheim, CA

July 12-14, 2017
Chicago, IL

October 23-25, 2017
New York, NY

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP231

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

Senior Auditors; Internal and External Auditors; Audit Managers

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

November 7-9, 2016
Dallas, TX

March 6-8, 2017
New York, NY

September 18-20, 2017
San Francisco, CA

November 27-29, 2017
Boston, MA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP234

Process Flow 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

Audit Directors and Managers; Internal, External and Information Technology Auditors

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. **IA's Role and Identity**

SCHEDULE

October 17-19, 2016
Washington, DC

April 3-5, 2017
Chicago, IL

August 14-16, 2017
Washington, DC

November 27-29, 2017
Anaheim, CA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP311

OAP315

Lean Six Sigma Skills for Auditors

Acquiring the Essential Six Sigma Skills for Process Improvement

Seminar Focus and Features

Initially designed as a set of practices to improve manufacturing processes and eliminate defects, Six Sigma focuses on consistency, quality and constant improvement, the very same goals that internal auditors promote during their audits and consulting projects. A data-driven, quality improvement initiative, Six Sigma provides internal auditors with an invaluable tool to improve processes and implement and measure the effectiveness of internal controls.

Throughout this two-day course you will learn what Six Sigma is all about and find out how to leverage its principles for better internal controls. You will identify critical operational issues and discover how to develop better recommendations that will lead to higher operational efficiency and effectiveness. You will go through the phases of Six Sigma and cover project scope and goals, uncovering the root cause of defects and applying metrics to determine the effectiveness of performance levels. You will see for yourself how Six Sigma can enhance your ERM and GRC processes while reducing costs and wasted time. Throughout this practical seminar, you will use a variety of tools to apply Six Sigma concepts and you will return to your office with Six Sigma skills that will position you to add immediate value to your organization.

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 Auditors; IT Auditors; Senior and In-Charge Auditors; Audit Managers and Directors; and Audit Team Leaders

What You Will Learn

1. **Six Sigma: Terminology and Key Concepts**
2. **The "Define" Phase**
3. **The "Measure" Phase**
4. **The "Analyze" Phase**
5. **The "Improve" Phase**
6. **The "Control" Phase**
7. **Process Mapping**
8. **Project Management and Team Building**
9. **The 14 Principles of the Toyota Way**

SCHEDULE

March 9-10, 2017
New York, NY

June 8-9, 2017
San Diego, CA

September 21-22, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAP315

OAP362 **NEW!**

How to Perform and Benefit from a Peer Review

Knowledge and Techniques to Conduct a Quality Assessment Review

Seminar Focus and Features

The International Standards for the Professional Practice of Internal Auditing requires every internal audit department or activity to have either an external Quality Assessment Review (QAR) or a Self-Assessment review with an external validation by an independent reviewer at least once every five years. This two-day seminar will provide what you need to know to prepare for and to undergo an external quality assessment review and will explain how to conduct a self-assessment as outlined by the IIA Standards. Attendees will gain an understanding of how a QAR can benefit the internal audit activity; learn about the various review methodologies that are available; and discuss the important decisions that arise when preparing an internal audit department for a review.

The course also examines the Professional Practices Framework, including the International Standards for the Professional Practice of Internal Auditing and the external assessment requirements that are mandated in order to be in compliance with the IIA Standards. You will explore best practices in internal auditing and state-of-the-art assessment techniques and practices for conducting a QAR. You will work through a case study developed from dozens of actual QARs that will highlight how the process works and how to apply the IIA Standards when conducting a review.

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Chief Audit Executives, Audit Directors and Managers; Internal Auditors who need an understanding of the IIA Standards in order to be on an external review team, or an internal self-assessment team, and those responsible for outsourced internal audit activities

What You Will Learn

1. **Peer Review Requirements under the IIA Standards**
2. **What Is a Peer/Quality Assessment Review?**
3. **Review Methodologies for Internal Auditing**
4. **The IIA Professional Practices Framework**
5. **Preparing for the Assessment**
6. **Fieldwork**
7. **Reporting the Opinion**
8. **A Survival Checklist for Chief Audit Executives**
9. **Best Practices in Value-Added Internal Auditing**
10. **Hands-On Case Study**

SCHEDULE

October 3-4, 2016
Orlando, FL

March 9-10, 2017
Orlando, FL

June 15-16, 2017
New York, NY

October 16-17, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAP362

OAP320 NEW!

Six Sigma White Belt for Auditors

Using Introductory Efficiency and Quality Techniques for Process Improvement

Seminar Focus and Features

Six Sigma provides internal auditors, risk and security professionals, project managers and business process owners with a set of invaluable tools to improve processes and implement and measure the effectiveness of internal controls as discussed in the Lean Six Sigma Skills for Auditors seminar. Anyone responsible for business processes, conducting control self-assessments, or overseeing risk assessments can benefit from following a proven methodology like Six Sigma. Benefits to the enterprise include process automation, increased efficiency, streamlined processes and removal of wasteful and unnecessary activities.

Throughout this three-day course, you will expand on the basic concepts of Lean Six Sigma and discuss and practice techniques to leverage its principles for better internal controls. Through instruction and case studies we will identify critical operational issues and, as teams, develop recommendations that will lead to higher operational efficiency and effectiveness. You will review the phases of the DMAIC process focusing additional attention on the Define phase. Upon completion of the course project, participants are invited to participate in the White Belt Certificate Exam which consists of 30 multiple choice questions. Certificates will be awarded to those with a score of 23 or greater.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or equivalent experience and Lean Six Sigma Skills for Auditors OAP315 or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operational, Business Applications, IT and External Auditors, Project Managers, Information Security Professionals, Risk Management Professionals and Business Leaders who want a deeper understanding of Six Sigma from the assurance perspective

What You Will Learn

1. **Six Sigma: Review of Terminology and Key Concepts**
2. **The "Define" Phase**
3. **The "Measure" Phase**
4. **The "Analysis" Phase**
5. **The "Improve" Phase**
6. **The "Control" Phase**
7. **Six Sigma Project Participation**

SCHEDULE

February 13-15, 2017
Orlando, FL

July 24-26, 2017
Boston, MA

October 16-18, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP320

OAP321 NEW!

Six Sigma Yellow Belt for Auditors

Using Introductory Efficiency and Quality Techniques for Process Improvement

Seminar Focus and Features

Six Sigma allows organizations to assess their current business processes and find new and innovative ways to reduce redundancies while embracing automation. Anyone can improve processes and implement and measure the effectiveness of internal controls using the proven Six Sigma tools and techniques. This seminar is the second in our Six Sigma series and focuses on the execution of the DMAIC methodology.

Throughout this three-day course you will expand on the basic concepts of the Six Sigma White Belt for Auditors course and discuss and practice techniques to leverage its principles for better internal controls. Through instruction and case studies we will identify critical operational issues and, as teams, develop recommendations that will lead to higher operational efficiency and effectiveness. The exercise will allow attendees to develop an appropriate project scope and goals, uncover the root cause of defects, and apply metrics to determine the effectiveness of performance levels. Upon completion of the course project, participants are invited to participate in the Yellow Belt Certificate exam, which consists of 50 multiple choice questions. Certificates will be awarded to those who score 38 or greater on the exam.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or equivalent experience; Lean Six Sigma Skills for Auditors (OAP315) and Six Sigma White Belt for Auditors (OAP320)

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operational, Business Applications, IT and External Auditors, Project Managers, Information Security Professionals, Risk Management Professionals and Business Leaders who want a deeper understanding of Six Sigma from the assurance perspective

What You Will Learn

1. **Six Sigma: Review of Terminology and Key Concepts – White Belt Review**
2. **The "Define" Phase**
3. **The "Measure" Phase**
4. **The "Analyze" Phase**
5. **The "Improve" Phase**
6. **The "Control" Phase**
7. **Project Team**
8. **Basic Tools and Statistics**
9. **Six Sigma Project Participation**

SCHEDULE

October 3-5, 2016
Orlando, FL

March 6-8, 2017
Orlando, FL

August 14-16, 2017
Boston, MA

November 13-15, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP321

OAP420 NEW!

Six Sigma Green Belt for Auditors

Using Advanced Efficiency and Quality Techniques for Process Improvement

Seminar Focus and Features

Organizations that apply Six Sigma techniques into their business processes reduce waste and improve throughput when properly deployed. Auditors can use this methodology to improve the auditing process, assess the effectiveness of an organization's Process Improvement team or simply assess the effectiveness and efficiency or any business or technology process. This seminar is the third in our Six Sigma series and focuses on the tools of Six Sigma.

Throughout this five-day course you will expand on the concepts of the Six Sigma Yellow Belt course and discuss and practice techniques to leverage its principles for better internal controls. Through instruction and case studies we will identify critical operational issues and, as teams, develop recommendations that will lead to higher operational efficiency and effectiveness. You will review the phases of Six Sigma and cover project scope and goals, uncover the root cause of defects, and apply metrics to determine the effectiveness of performance levels. Throughout this practical seminar, you will use a variety of tools to apply Six Sigma concepts. After the course, attendees will be given six months to complete a Six Sigma project with $100,000 or more in cost savings.

At any time after the course attendees can take a 100 question online exam. A Green Belt for Auditors Certificate will be issued to those who complete the exercise and have a test score greater than 75.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or equivalent experience; Lean Six Sigma Skills for Auditors (OAP315) and Six Sigma White Belt for Auditors (OAP320) and Six Sigma Yellow Belt for Auditors (OAP321)

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operational, Business Applications, IT and External Auditors, Project Managers, Information Security Professionals, Risk Management Professionals and Business Leaders who want a deeper understanding of Six Sigma from the assurance perspective

What You Will Learn

1. Six Sigma: History and Overview
2. Preparing for Analysis (Define and Measure)
3. Root Cause (Analysis)
4. Control Charts
5. Process Capability
6. Tools and Terms
7. Applications
8. Six Sigma Project Participation

SCHEDULE

December 12-16, 2016
Orlando, FL

May 1-5, 2017
Orlando, FL

September 18-22, 2017
Boston, MA

December 11-15, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2895 **40 CPEs**

Web: misti.com/OAP420

OAG260

Auditing Networks for Non-IT Auditors

Eliminating the FUD from Auditing Practices

Seminar Focus and Features

Most auditors do not audit networks. Why? Because they do not understand them or perceive these audits are time-consuming and highly technical. Surprise! They are not. In fact, you can audit dynamic networks in less than two weeks with no prior technical knowledge. Don't be a statistic. Don't be the next "We were hacked!" story to show up in the headlines. This two-day course will aid you in eliminating the Fear, Uncertainty and Doubt (FUD) from auditing practices.

Non-IT auditors will want to come to this course to learn proven techniques for understanding, assessing and testing network security and configurations quickly and achieve high-success results. And all of this will be based on risk, not just a "do everything possible" approach some "experts" advocate. Stop avoiding this technology! Attend this course to learn how you, an auditor without deep, technical expertise, can actually help improve the security of your organization's systems through a basic, and easy to learn, technology understanding that supplements your audit expertise.

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Operational, Business Application, Information Technology and External Auditors; Audit Managers and Directors; Information Security professionals

What You Will Learn

1. Recent Hack Attacks
2. The Layers of Network Security
3. Network Security Policies
4. Firewalls
5. Intrusion Prevention Systems
6. Intrusion Detection Systems
7. Anti-Virus Software
8. Identify Access Management
9. Wireless
10. Data Transmission Encryption and Certificate Authorities
11. Encryption of Data-At-Rest
12. Networks Physical Security
13. Conducting Network Penetration Tests
14. If You Were Hacked, Would You Know?
15. Network Security Resources

SCHEDULE

November 2-3, 2016
San Francisco, CA

February 9-10, 2017
San Francisco, CA

May 18-19, 2017
Washington, DC

September 28-29, 2017
Chicago, IL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAG260

The Audit Leadership Institute

A Unique Executive Development Program

Seminar Focus and Features

What does it take to successfully lead a risk-based audit department in a fast-paced, changing environment? In this five-day program we will explore the new directions, habits and practices of highly effective audit leaders. We will look at the leadership styles that leading audit executives use, how they solve problems and how they inspire their staff. The seminar 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 program will also cover some practical and tactical skills all top audit leaders need to develop, such as investigating fraud, assessing risk, using data analytics and keeping up with evolving technology.

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

Newly appointed CAEs, Vice Presidents, Directors, Managers, Supervisors and other members of the audit management team who want to learn new approaches to being a leader in today's dynamic internal audit climate

What You Will Learn

1. **What It Takes to Be an Audit Leader of a World-Class Audit Function in Today's Turbulent Times**
2. **The Greatest Challenges Facing Audit Leaders in the Next Three Years**
   - embracing the latest technology changes
   - finding and retaining the best talent
   - identifying and addressing only the most significant risks and key controls
   - benefiting from data mining and data analytics
3. **Changing Dynamics of the Manager's Position**
   - increasingly important need to understand the business and their risks
   - keeping abreast of emerging risks such as cybercrime, social responsibility, etc.
4. **The ERM Benefits of a Robust GRC Program**
   - integrating risks identified in SOX, compliance and fraud into your risk model
   - prioritizing governance and entity level controls
5. **Leading a Successful Risk-Based Audit Department**
6. **Balancing the Expectations of Multiple Customers**
   - concentrating on high-impact risks
   - partnering with external auditors, compliance officers and the ERM function
   - helping executive management meet their business goals
7. **People, People, People: Getting the Most Out of Multiple People Resources**
   - maximizing your investment in co-sourcing, outsourcing and insourcing
   - rethinking where we find and then develop new talent
   - building the team that can address your ERM
8. **The Art of Effective Audit Leadership: Is Your Style Helping or Hurting?**
9. **How to Be a Trusted Advisor: Using Influence and Building Integrity**
   - identify the five behaviors of trusted advisors
   - assessing your audit situation to identify decision-makers, stakeholders and other influencers
   - identifying your preferred influencing style and exploring different ones
10. **Using Conflict Resolution and Negotiation Techniques for Sustained Organizational Change**
    - defining audit's role in creating sustained organizational change
    - recognizing the critical conversations and circumstances that lead to conflict
    - managing existing conflicts using three methods
11. **Enhancing Audit Committee and Senior Management Relations and Communication**
    - building and maintaining great audit and executive committee relationships
    - clarifying the roles of the board and the Audit Committee, and Internal Audit's interactions with each
    - defining above- and below-the-line activities
    - best practices for boards and how your organization compares
    - balancing the detailed and summary information you communicate
    - delivering high-impact presentations to the audit and executive committees
12. **Developing Audit Reports That Foster Change**
    - using an attention-getting, reader-friendly layout
    - communicating audit and SOX concerns for maximum impact and efficiency
    - identifying opportunities for expanded and enhanced reporting in a post-SOX environment
13. **Enhancing Bench Strength and Building the Right Team**
    - identifying the competencies needed for a risk-based department
    - attracting and retaining change agent-oriented auditors
    - using "the nine boxes" to develop succession plans and evaluate performance
    - leveraging MBO programs to build critical skills needed for succession planning
14. **Ensuring Your Department is Maximizing Its Proactive Role in Preventing and Detecting Fraud**
    - using effective methods for fraud detection and investigation
    - ensuring success through collaboration with other functions involved in mitigating fraud
15. **The Audit Leader's Role in Developing and Implementing a Fraud Risk Assessment**
    - developing the comprehensive approach
    - effectively matching resources to risks
16. **Effectively Reporting Fraud Risks to the Audit Committee**
    - making the investment in anti-fraud programs successful
17. **Implementing a Fraud Risk Management Strategy**
    - identify elements of a comprehensive framework
    - resources for successful implementation
18. **The Audit Leader's Role in a Fraud Investigation**
    - managing the expectations of senior management
    - identify the best roles in the investigation process
19. **Making Your Department more Fraud Savvy**
    - laws and regulations impacting fraud risk management
    - optimizing tools and techniques for fraud training
20. **Eliminating What You Do Not Need: Working Smarter, Not Harder**
21. **Transforming the Audit Process, Increasing Effectiveness and Efficiency**
    - identifying significant risks earlier in the audit process
    - eliminating low-risk, low probability steps
    - spending more time in the planning process identifying key controls
22. **Incorporating Best Practices into Your Audit Processes**

SCHEDULE

TBD

Tuition $3495 **40 CPEs**

Web: misti.com/OAM510

The CAE Master's Program

A Blueprint for the Chief Audit Executive

Seminar Focus and Features

The CAE Master's Program brings together a team of thought leaders and practitioners in internal audit companies for an intensive, three-day program. The gathering blends practical management techniques and skills with the latest management theories and strategies to help CAE's position themselves and their teams as valued and effective business partners.

This unique, executive education program has been designed to:

1. Create an environment where experienced audit leaders can learn from each other and exchange successful strategies and ideas.
2. Give CAEs a learning experience that combines strategy and theory from top internal audit faculty.
3. Provide an intimate, interactive setting for a high-quality program in a format that fits your busy schedule.

The focus in on audit leadership. The sessions are rigorous. In short, we bring you the knowledge and strategies you need in a way that fits both your schedule and your budget.

Prerequisite: Must be a senior audit executive

Advance Preparation: None

Learning Level: Advanced

Field: Business Management & Organization

Delivery Method: Group-Live

Who Should Attend

CAEs and other audit executives, managers and directors looking to reach the upper echelon of leading an IA department; past attendees of The Audit Leadership Institute

What You Will Learn

1. **Internal Audit: The Big Issues Today and Tomorrow**
   - leveraging and harnessing technology
   - prioritizing strategies that add value
   - sustaining great relationships with the Audit Committee and the C-Suite
   - developing a true risk-based team for today and tomorrow
   - addressing only the most significant risks and key controls
2. **Internal Audit as a Proactive Change Agent**
3. **Developing the Strategic Vision**
   - developing viable action plans to achieve strategic goals
   - identify the potential hurdles that need to be overcome
   - establishing departmental objectives for the next five years
4. **Tools Needed to Add Value to the Audit Committee and C-Suite**
   - reporting out: solutions for dealing with high profile situations
5. **Defining the Internal Audit Value Proposition**
   - tools for creating meaningful value propositions
   - discuss how others have implemented high-impact value propositions
   - identify the components of high-impact value propositions
   - determine how to measure the usefulness of value propositions
   - explore the critical role of the Internal Audit value proposition
6. **Incorporating the Updated COSO Framework into Your Strategic Plan**
7. **People, People, People - Focusing on Human Capital**
   - innovative ways to find A-level talent
   - define the components of a world-class team
   - manage non-performers and under-performers
   - succession planning
   - build bench strength
8. **Lessons Learned - Refining the Take-Away Battle Plan to Deliver Results**
9. **Reporting Out: Ideas on the Internal Audit Value Proposition**
10. **Fostering a Partnership with Internal Audit and Corporate Compliance to add Value to the Audit Committee and C-Suite**
11. **Ways to Be Effective and Efficient without Compromising Quality**
    - techniques for promoting sound auditing and risk management in post-merger/acquisition environment
    - refine and leverage the ERM process
    - leveraging technology
    - expand risk coverage without increasing the staff
12. **Being the Trusted Advisor and Go-To Business Partner**
    - techniques for managing global relationships
    - move the needle to affect your organization's risk management culture
    - tools for assessing the organizational culture
    - hone relationship with Executive Committee and the Audit Committee
13. **Building the Take-Away Game Plan**
    - eliminating low risk, low probability audits and audit steps
    - knowing the business
    - integrating compliance, risk, fraud and information security functions
    - having the right audit process

SCHEDULE

June 12-14, 2017
Chicago, IL

Tuition **28 CPEs**

$3295 Early Price (until 4/16/17)
$3495 Regular Price

Web: misti.com/OAM590

OAG520 NEW!

Advanced Internal Audit Masterclass

Advanced and Innovative Internal Audit Strategies for Audit Directors and Managers

Seminar Focus and Features

This training kicks off with a review of Internal Auditing fundamentals, including reviewing the roles and responsibilities of the entire Internal Audit department staff and the standards and guidance of Internal Auditing. The course is designed to facilitate discussion and dialogue while debating challenges, ideas and strategies to take your IA department to the next level and achieve excellence in fulfilling your mission. We will focus on strategy development and the importance of alignment as we navigate through the challenges, threats and opportunities in an ever-changing environment. Participants will gain a clear understanding of the role, responsibilities and the value added as an IA department and organization; then look ahead to the future to determine our next best course of action. We will work on clarifying IA's purpose, brand, identity, mission and vision to assist participants in the creation of a tailored strategic road map.

Following the discussion of strategy development, participants will shift focus to strategy translation and execution. We will examine the importance of alignment and explore helpful and necessary tools to help build an action plan that leads to a more outstanding internal audit department. The goal of the personal, tailored action plan is to help participants assess where they are now, where they want/need to go and map out a plan to get there.

Prerequisite: Internal Audit School (OAP301) or equivalent experience

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Internal Audit Directors, Managers and Supervisors from private, public and not-for-profit sector

What You Will Learn

1. **Fundamentals of Internal Audit**
2. **Strategy Development**
3. **Strategy Translation and Execution**
4. **Other Internal and External Factors, Ideas and Strategies to Consider**
5. **Putting it all Together - Developing a Tailored Action Plan**

SCHEDULE

September 26-28, 2016
New York, NY

April 3-5, 2017
Boston, MA

August 2-4, 2017
Washington, DC

November 13-15, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAG520

OAM302

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 Managers, Directors and Supervisors

What You Will Learn

1. **Understanding IT Risks**
2. **Taking the Mystery Out of Information Technology: Battling the Buzzwords**
3. **Key IT Infrastructure Risks and Controls**
4. **Business Application System Risks and Controls**
5. **Assessing IT Governance**
6. **Developing the IT Audit Plan**

SCHEDULE

November 2-3, 2016
San Francisco, CA

March 9-10, 2017
Chicago, IL

August 10-11, 2017
Washington, DC

October 2-3, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAM302

"Very informative. Instructor very knowledgeable. He made it interesting."

Josiah Kuo,
IA/J-SOX Compliance Manager,
Roland DGA

OAM401

Managing the Internal Audit Department

Directing and Managing a Risk-Based, IA Department That Adds Real Value to the Organization

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 IA 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 IA, you will cover setting attainable objectives and goals; reacting to changing risk/control relationships; marketing IA's services; structuring the audit department; the annual audit planning process; co-sourcing smarter; and more.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or 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 Managers, Directors and Supervisors

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. IA's Role in Recent High-Profile Situations and What Went Wrong – Lessons Learned

SCHEDULE

December 5-7, 2016
San Francisco, CA

March 13-15, 2017
Orlando, FL

June 5-7, 2017
San Diego, CA

September 25-27, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAM401

OAM425

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: Managing the Internal Audit Department (OAM401) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Audit Managers, Directors, Senior Auditors and Audit Team Leaders

What You Will Learn

1. From Managing to Leading
2. Essential Leadership and Management Skills
3. Hiring and Motivating Employees
4. Time, Stress and Priorities Management
5. Communication Skills, Team Building and Conflict Management
6. Common Management Mistakes
7. Training and Mentoring Programs
8. Leading Change
9. Global Auditing

SCHEDULE

November 30-December 2, 2016
New York, NY

February 27-March 1, 2017
Las Vegas, NV

May 22-24, 2017
Boston, MA

October 16-18, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAM425

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

Financial, Operational, IT, Internal and External Auditors; Audit Managers; Corporate Attorneys; Information Security Professionals; Risk Management Personnel and Line Managers who need to gain an understanding of the growing risks of fraud

What You Will Learn

1. **Understanding How Fraud Occurs**
   - integrating the fraud theory into your audit
   - incorporating the fraud audit matrix
   - comparing approaches: internal audit, fraud audit and forensic investigation
   - the fraud triangle: opportunity, pressures and rationalization
   - identifying who commits fraud
   - fraud in plain English
   - identifying what actually constitutes fraud in your organization
   - how perpetrators conceal fraud
   - the premise of concealment and concealment strategies
   - conversion: how perpetrators benefit from the fraud scheme
   - identifying types of conversion and understanding different audit and industry strategies
2. **Building Fraud Scenarios**
   - understanding the fraud risk structure
   - the inherent fraud schemes in every business system
   - how to build fraud scenarios for individual audit programs
3. **Preparing a Business Process Fraud Risk Assessment for Audit Programs**
   - using the drill-down approach to identify scheme variations for each business system
   - how to link fraud risks for each business process to your control structure
   - establishing a score for mitigation of fraud risk by internal controls
   - how to link the control fraud scores to the audit response
4. **Incorporating Fraud Risk Assessment into the Audit Program**
   - fraud scheme approach
   - fraud opportunity approach
   - techniques to assess fraud risk
   - internal controls and fraud risk
   - audit response and fraud risks
   - individual and aggregate fraud risks
   - business risk factors
5. **Integrating Fraud Testing into Your Audit Program**
   - using red flags to identify fraud
   - how to build and analyze red flags for specific schemes
   - fraud data analysis: approaches and strategies
   - how to build the fraud data profile: the step approach for data mining
   - identifying the response to fraud based on the fraud risk assessment: control vs. fraud approach
   - incorporating fraud steps into the audit program
   - how to design fraud audit procedures to pierce the concealment strategy
   - linking the audit program to the risk assessment
   - sampling designed to locate fraud
   - testing and evaluating the design of your anti-fraud controls
   - identifying suspicious transactions through fraud audit procedures
   - writing fraud audit findings and the legal considerations
6. **Interviewing for Fraud in the Audit Process**
   - using the fraud scenario approach
   - the five types of questions
   - preparation for the interview process
   - managing the reluctant witness
   - connecting the fraud scenario to the illegal act
7. **Internal Controls and Fraud**
   - how controls are related to the fraud theory
   - fraud control: prevention, detection, deterrence, prosecution and approval
   - fraud prevention programs
   - how to design controls to minimize fraud
   - managing fraud costs
   - developing fraud awareness programs
8. **Misappropriation of Assets**
   - disbursement fraud schemes
   - purchasing fraud schemes
   - fraud in payroll and HR
   - contract fraud schemes
   - fraud in revenue and cash receipts functions
   - theft of inventory, equipment and assets
   - travel expense fraud schemes
9. **Financial Statement Fraud**
   - fraud in the revenue cycle
   - inventory fraud schemes
   - expenditure fraud schemes
   - journal entry fraud schemes
   - management fraud: incentive, opportunity and rationalization
10. **Professional Standards**
    - Sarbanes-Oxley and PCAOB
    - SAS No. 99
    - Institute of Internal Auditors
    - Yellow Book
    - current surveys and reports on fraud
11. **Fraud Investigation**
    - identifying resources to conduct an investigation
    - focusing on fraud theory and development
    - using private investigators
    - types of interviews and the appropriate approach
    - understanding the interview methodology
    - legal considerations when conducting an interview
    - appropriate collection and analysis of documentation
    - forensic examination of documentation
    - individual rights during investigations
    - how the legal system works
    - types of evidence
12. **Interviewing: Admission-Seeking and Legal Elements**
    - initial steps to securing the admission
    - obtaining the oral confession
    - what are the legal considerations

SCHEDULE

November 14-17, 2016
San Francisco, CA

May 15-18, 2017
Washington, DC

June 12-15, 2017
New York, NY

August 21-24, 2017
Anaheim, CA

October 23-26, 2017
New York, NY

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/OAF201

OAF411

Advanced Fraud Audit School

Advanced Workshop on Using Fraud Detection Procedures

Seminar Focus and Features

In this four-day seminar you will work on two real-life case studies and simulate every aspect of a fraud audit. You will start with the fraud risk identification by examining documents, using background reports to search for clues, researching vendor existence and leveraging advance techniques to obtain information to corroborate suspicions of fraud. At the conclusion of the class you will understand how to identify the red flags which warrant an internal investigation.

You will learn how to investigate company fraud hotline tips, determine the credibility of an allegation and apply document analysis procedures to actual fraud documents. You will get tips on developing data mining techniques, conduct a fraud penetration analysis and drill down to the specifics of such fraudulent activities as disbursement fraud and bribery and corruption. The course material provides sample reports, fraud risk structure documents, fraud website listings and many more reference tools.

You will build fraud audit plans, prepare written reports, conduct mock interviews and prepare your work papers for court. This course starts with the audit and concludes with you uncovering fraud in the classroom.

NOTE: *A laptop will assist in completing exercises but is not required.*

Prerequisite: Fraud Auditing Boot Camp (OAF201) or Fraud Testing: Integrating Fraud Detection into Your Audit Program (OAF301) or equivalent experience

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operational, IT and External Auditors; Audit Managers; Fraud Investigators and Managers; Corporate Attorneys; Risk Management personnel; and Information Security professionals

What You Will Learn

1. Understanding How Fraud Occurs
2. Conducting the Fraud Audit
3. Fraud Audit: Bribery and Corruption
4. Fraud Audit: Disbursement Fraud Schemes
5. Fraud Data Mining
6. Writing Your Fraud Report
7. Company Hotlines
8. Performing the Internal Fraud Investigation
9. Legal Elements of Fraud
10. Interviewing/Interrogation
11. Preparing Your Work Papers
12. Critical Fraud Policies

SCHEDULE

April 25-28, 2017
New York, NY

July 10-13, 2017
Chicago, IL

October 10-13, 2017
Boston, MA

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/OAF411

OAF301

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

Financial, Operational, Information Technology and External Auditors; Audit Managers; Corporate Attorneys; Business Managers; Quality Assurance, Risk and Compliance Managers; and Information Security Professionals

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

October 17-19, 2016
New York, NY

May 22-24, 2017
New York, NY

July 17-19, 2017
Boston, MA

October 2-4, 2017
San Diego, CA

December 4-6, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAF301

OAF315

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

Financial, Operational, Internal, IT and External Auditors; Audit Managers; Fraud Investigators and Managers; Risk and Compliance Managers and Officers; Information Security Professionals

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

September 26-28, 2016
Chicago, IL

December 12-14, 2016
Orlando, FL

June 5-7, 2017
San Diego, CA

August 14-16, 2017
New York, NY

September 25-27, 2017
Chicago, IL

December 18-20, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAF315

OAP215

Data Mining for Auditors

A Logical Approach to Continuous Auditing and Governance

Seminar Focus and Features

To meet the challenges of the 21st century, it is necessary for internal audit to reboot and become closely aligned with the business issues confronting organizations today. A logical audit presence driven by data coupled with continuous/continual and virtual audit is a practical strategy for achieving this goal.

In this three-day seminar you will learn how to effectively use data as the driver for multiple audit functionalities, from risk assessment to highly effective visual-based audit reports. You will learn which data to mine to minimize audit resources and maximize audit and business outcomes by delivering business-focused recommendations that will bring about constructive change. In addition, you will learn how to create and use progressive system-centric/data-centric audit tools and oversight strategies and techniques for performing continuous auditing that will enable your organization to be best-in-class in today's global competitive market place.

NOTE: *You are encouraged to bring a laptop to perform a number of hands-on exercises involving data and how it should be applied to your organization.*

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Risk and Compliance Managers; Audit Directors and Managers; Financial, Operational and IT Auditors; Key Operational personnel

What You Will Learn

1. Aligning the Audit Function with the Business
2. Defining Data Mining and Its Uses
3. Maximizing the Use of Data
4. Data Analysis Methodologies: Logically Focusing the Audits on Critical Business Concerns
5. Defining a Continuous Audit Process for Maximum Effectiveness
6. Changes Brought About by Data-Centric Auditing
7. Focusing Reporting on Outcomes Not Outputs
8. Data-Centric Exercises

SCHEDULE

December 12-14, 2016
Orlando, FL

March 20-22, 2017
San Diego, CA

August 28-30, 2017
New York, NY

October 9-11, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP215

OAF211

The Auditor's Guide to Money Laundering

Identifying and Preventing Money Laundering

Seminar Focus and Features

Billions of dollars are laundered annually throughout the world. Employing effective internal controls and audits are two key measures to prevent money laundering from taking place in your organization. In this two-day seminar, you will review the domestic and international regulations surrounding the worldwide anti-money laundering efforts. You will gain an understanding of the money laundering basics: how it's done, how to identify common red flags and what measures your organization should have in place to prevent money laundering from taking place. Real-world case studies, as well as detailed audit procedures, will provide takeaways that are practical and useful in the fight against money laundering. A must for any auditor involved in the audit process for BSA/OFAC compliance, as well as auditors looking to stay current on both domestic and international regulations.

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

Financial, Operational, Internal, IT and External Auditors; Audit Managers; Fraud Investigators and Managers; Risk and Compliance Managers and Officers; Information Security Professionals

What You Will Learn

1. Money Laundering Defined
2. US Regulations
3. International Regulations and Initiatives
4. Money Laundering 101 – How Is It Done?
5. BSA/AML Compliance Programs
6. OFAC Compliance Programs
7. BSA/OFAC for Non-Bank Entities
8. Red Flags of Money Laundering
9. Auditing for Money Laundering
10. Money Laundering Case Studies

SCHEDULE

November 3-4, 2016
New York, NY

March 9-10, 2017
San Francisco, CA

June 15-16, 2017
New York, NY

November 2-3, 2017
Washington, DC

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAF211

OAF340

Bribery and Corruption: FCPA and UK Bribery Act Compliance

A Comprehensive Guide to Auditing the Compliance Program and Controls

Seminar Focus and Features

In 2010, the Securities and Exchange Commission's dedicated Foreign Corrupt Practices Act (FCPA) unit levied a record $1.8 billion in FCPA related violations. The Department of Justice and UK Serious Fraud Office expect the number of FCPA and UK Bribery Act related prosecutions to increase. Clearly, the question is not whether more government investigations will occur, but how much will it cost your organization. Companies must identify high risk activities, business opportunities and business partners while focusing real effort on mitigating risk.

Over the course of this two-day seminar, we will focus on the law, corruption risk, internal controls and audit and investigation strategies to ensure your company can demonstrate corporate compliance. Discussion points will be based on actual DOJ enforcement cases and case studies will be used to reinforce course material. At the conclusion of this seminar, attendees will be able to conduct a comprehensive FCPA or Bribery Act based audit.

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

Fraud Investigators and Managers; Financial, Operational, Internal, IT and External Auditors; Audit Managers; Risk and Compliance Managers and Officers; Information Security Professionals

What You Will Learn

1. Understanding How Corruption Occurs
2. Introduction to Corruption Legislation
3. Preparing the Corruption Risk Assessment
4. Right Internal Controls to Combat Bribery and Corruption
5. Conducting the Corruption Audit
6. Conducting the Corruption Investigation
7. Corruption Schemes in Your Purchasing Cycle
8. Corruption Schemes in Your Revenue Cycle

SCHEDULE

December 15-16, 2016
Orlando, FL

June 8-9, 2017
San Diego, CA

December 7-8, 2017
Orlando, FL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAF340

OAF403 NEW!

Fraud in Financial Accounts and Statements

The Fraud Scenario Approach to Detecting Fraud

Seminar Focus and Features

In this two-day seminar, you will learn the most common fraud schemes used to misstate key financial accounts in your financial statements. The course will cover fraud risk assessment, fraud data analytics and how to integrate fraud testing into your audit programs. Learn how management has concealed the fraud in financial accounts and then tricked the auditors. Learn how to build the red flag testing into your audit program. Class exercises are used in each chapter to reinforce the learning objectives. At the conclusion of the seminar, you will be able develop your fraud audit program for key financial accounts.

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

Who Should Attend

Internal and IT Auditors with more than two years of financial audit experience, experienced auditors who need to know more about GAAP and fraud in financial reporting

What You Will Learn

1. Understanding How Fraud Occurs
2. Preparing the Fraud Risk Assessment for Financial Accounts
3. Understanding Key PCAOB Requirements
4. Fraud Testing Methodologies
5. Revenue Recognition Manipulation
6. Journal Entry Testing
7. Asset Manipulation Schemes
8. Common Asset Misappropriation Schemes
9. Study of the Financial Statement Fraud Classics

SCHEDULE

October 20-21, 2016
New York, NY

May 1-2, 2017
New York, NY

July 24-25, 2017
Boston, MA

October 5-6, 2017
San Diego, CA

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAF403

ITF221 NEW!

Combating Computer Fraud

Methodologies to Protect the Organization from Internal and External Computer Fraud Threats

Seminar Focus and Features

Any fraud committed with the aid of, or directly involving a computer or network is considered computer fraud. It's no wonder then that in today's highly automated business environment, foiling computer-based fraud has become a top priority as skilled computer experts, international criminal organizations and even seemingly honest employees steal identities, re-route data for personal gain, and alter data for fraudulent purposes…all with far-reaching and costly consequences.

In this three-day seminar you will examine the key risks surrounding computer-based fraud and explore the "who, what, and how" of this pervasive crime. You will investigate specific IT controls that must be in place to reduce the risk of computer fraud including logical access controls, reduced privileged access, application change management, network controls, encryption, application system controls and benefit from real-life examples of their effectiveness. You will review a range of fraud studies with control recommendations from sources including the Association of Certified Fraud Examiners. You will leave this high-impact seminar with a game plan for reducing computer fraud risks in your organization.

Prerequisite: IT Auditing and Controls (ITG101), IT Audit School (ITG121) or equivalent experience
Advance Preparation: None
Learning Level: Basic
Field: Auditing
Delivery Method: Group-Live

Who Should Attend

Internal and External Auditors (IT, Business, Financial), Audit Management, Risk Management

What You Will Learn

1. Risk Assessment and Audit Planning
2. Fraud Overview
3. Fraud Risks
4. Computer Fraud Exposures
5. IT Controls to Reduce Fraud Risk
6. Logical Access Controls
7. System Software Security
8. Change Management
9. Network Perimeter Security
10. Physical Security
11. Application Controls
12. Auditing Outsourced IT Operations
13. Monitoring for Fraud
14. Evidence Gathering

SCHEDULE

November 7-9, 2016
New York, NY

July 17-19, 2017
Boston, MA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ITF221

Successful Audit Data Analytics

HANDS-ON

Getting the Most Out of Your CAATs Program

Seminar Focus and Features

In this three-day seminar attendees will learn everything needed about effectively integrating data analytics, or CAATs (Computer Assisted Audit Techniques), into an audit process. Attendees will learn how technology can be used to more efficiently and effectively achieve desired results and brainstorm analytics across most major business cycles. Learn how to progress from basic analytics into a fully automated/repetitive mode and learn the basics of Continuous Auditing. This seminar 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.

Whether you are in audit management, directing a team where you may never personally use the technology, or the person who will ultimately be performing data analysis techniques, this seminar provides critical experience. Participants in audit management will learn how to design effective strategies and programs to ensure sustainable results. Those who will play a hands-on role with analytics programs will get the opportunity to work on real-world scenarios with sample data files.

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

TOP 10 IN-HOUSE

Who Should Attend

Internal and External Auditors; Audit Managers, Directors and Executives; IT Auditors, Managers and Directors; QA personnel; IT Security Managers and Directors; CIOs; Consultants

What You Will Learn

1. **The Business Case for Audit Analytics**
   - industry benchmarks/guidance
   - challenges with traditional audit process
2. **Integrating Data Analytics Across the Audit Process**
   - enterprise risk assessment
   - fieldwork and testing
   - reporting
   - follow-up and monitors
3. **Pros and Cons of Common Data Analysis Tools**
   - generic: MS Excel, MS Access
   - business intelligence: Cognos, Spotfire, Business-Objects
   - Statistically-based: SPSS, SAS, WizSoft
   - IT-centric: SQL, Alteryx
   - specialized: SAP
   - audit-centric: ACL, IDEA, Arbutus
   - dashboarding: Tableau, QlikView
4. **Analytic Development Cycle**
   - program strategy and approach
   - data access and validation
   - coding/development
   - testing/QA
   - implementation and optimization
   - process differences for ad-hoc vs. continuous testing
5. **Planning for Data Access**
   - understanding various data access techniques
   - effective negotiation with IT
   - data verification procedures
   - data security and retention
6. **Exploring Data Access Options and File Types**
   - native database tools
   - ODBC
   - flat/delimited files
   - adobe PDF reports
   - unstructured data
7. **Common Analyses in Major Business Processes**
   - Record-to-Report (R2R)
   - Purchase-to-Pay (P2P)
   - Forecast-to-Stock (F2S)
   - Order-to-Cash (O2C)
   - Hire-to-Retire (H2R)
   - Process-to-Application (P2A)
8. **Advanced Analytic Design Techniques**
   - complex string comparisons
   - address comparisons
   - fuzzy matching techniques
   - trending
   - Benford's analysis
   - smarter sampling techniques
   - statistical and regression analysis
9. **Verifying Standard Data**
   - employee SSNs
   - vendor EINs
   - vendor TINs
   - zip codes/area codes/address abbreviations
   - credit card numbers
10. **Leveraging External Data Sources**
    - OFAC list
    - US Postal Service address standards
    - SIC codes
11. **Developing Appropriate Standards**
    - code documentation
    - requirements definition
    - data verification
    - QA and testing
    - security and archiving
12. **Making Analytics Repetitive**
    - scripting and automation
    - design considerations
    - automating data access
13. **Moving Towards Continuous Auditing**
    - strategy considerations
    - changes to data extraction and analytic logic
14. **Common Implementation Hurdles**
    - getting management buy-in
    - dealing with false positives
    - strategies for disparate systems
    - international issues
    - incongruent processes/policies
    - outsourced IT
    - external and cloud-based data
15. **People and Process Issues**
    - organizing the team
    - developing and maintaining skills
    - prioritizing analytics
    - measurement and KPIs
16. **Reporting and Interpreting Results**
    - presenting results in a meaningful way
    - analytic precision
17. **Advanced Topics and the Evolution of Analytics**
    - continuous monitoring
    - dashboard and visual analytics
    - score carding
    - predictive analytics
    - spatial relationships and mapping

SCHEDULE

October 24-26, 2016
New York, NY

November 29-December 1, 2016
Washington, DC

December 5-7, 2016
San Francisco, CA

January 30-February 1, 2017
Miami, FL

March 20-22, 2017
Las Vegas, NV

May 8-10, 2017
Boston, MA

July 24-26, 2017
Washington, DC

September 18-20, 2017
Chicago, IL

October 10-12, 2017
New York, NY

November 13-15, 2017
San Francisco, CA

November 29-December 1, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2595 **24 CPEs**

Web: misti.com/ITP250

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 IA 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

Audit Directors and Managers; Internal and External Auditors; Risk and Compliance Managers; and those charged with corporate governance responsibilities

What You Will Learn

1. **Risk-Focused Pronouncements and Publications**
   - ISO 3100 risk model
   - using the COSO ERM model as a baseline
   - ERM as presented in the UK/Ireland position paper: the role of internal audit
2. **Risk-Based Auditing**
   - the undercurrent of change in internal auditing
   - comparing and contrasting audit approaches
   - risk-based auditing benefits
3. **Risk Basics: What You Need to Know**
   - defining risk in business terms: essential for success
   - three key components of real risk assessment
   - the audit function and how it should be driven by risk
   - relating business risk and control failure
4. **Establishing a Framework for Risk Analysis**
   - alternative methods of determining risk in audit practice
   - using core business analysis to drive a top-down risk-based approach
   - centering risk assessment around the five key things a business does
5. **Aligning Key Business Risks with the Audit Universe**
   - key universal business risk categories: examples
   - prioritizing risk by critical functionality of the business
   - identifying the key business risks types in your organization
   - creating an effective risk-based audit plan
   - truly integrating the risk-based audit plan into the engagement-level risk assessment
6. **Objectively Driving the Audit Risk Assessment**
   - establishing a case for objective-based risk assessment
   - using data and proven information
   - making your analysis reactive rather than proactive
   - data analysis tools and how to use them for risk identification
   - interpreting data in the context of risk
   - types of analysis
7. **Identifying Risk Areas of Primary Concern**
   - financial: how to determine what's a risk and what's an exposure
   - operational: focusing on areas of real opportunity
   - IS/IT: determining the big payback areas of risk
   - regulatory: identifying the real points of risk focus
8. **Building an Inventory of Key Risk Metrics**
   - identifying essential key risk metrics
   - keying the metrics to ensure minimum data and maximum risk analysis
9. **Engagement-Level Risk Assessment**
   - engagement risk determined from the audit plan level
   - keying in on risk at the engagement level
   - focusing your evaluation on risk and control
   - building a risk-based audit program
10. **ERM: The New Risk Frontier**
    - understanding the role of IA in ERM
    - identifying new areas of audit concern and involvement
    - ERM and IA's symbiotic relationship
11. **Re-Engineering the Audit Process to Make It Truly Risk-Based**
    - questioning everything in the current audit process
    - utilizing multi-purpose risk-based audit tools
    - establishing a risk basis for everything you audit
    - focusing your audit on discovering root causal events
    - narrowing the scope of your audits to focus on only what is risky
    - creating a highly efficient risk-based reporting format
12. **Maximizing on Risk: Internal Audit Opportunity**
    - establishing a unique audit role that only you can fill
    - Provable Value Concept Auditing (PVCA)
13. **The Audit Spectrum**
    - practice today, tomorrow, the future
    - progressing toward risk-focused thought process
    - establishing a strategic risk vision
    - focusing on the tools of the future: self monitoring
14. **Marketing Risk-Based Auditing**
    - establishing the key advantages: how to get management buy-in
    - building the business case
    - formulating a transition plan
    - re-educating management and the Audit Committee

SCHEDULE

September 19-22, 2016
Chicago, IL

October 11-14, 2016
San Diego, CA

February 27-March 2, 2017
Phoenix, AZ

April 24-27, 2017
Boston, MA

June 19-22, 2017
Anaheim, CA

September 18-21, 2017
Chicago, IL

November 13-16, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/OAR201

OAR250

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 KRI's (Key Risk Indicators). 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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operations, IT and Regulatory Auditors; Public Accountants; governmental auditors; Internal and External Managers and Audit Executives; Risk and Compliance Managers

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 KRI's 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

February 9-10, 2017
San Francisco, CA

June 15-16, 2017
New York, NY

December 7-8, 2017
Orlando, FL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAR250

OAR321

Using Risk Assessment to Build Individual Audit Programs

A Methodology That Addresses Management's Business Concerns

Seminar Focus and Features

In this revealing 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 then 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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Audit Directors and Managers; Internal, External and IT Auditors; Risk and Compliance Managers; Operations Managers

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

November 14-16, 2016
Las Vegas, NV

March 13-15, 2017
Las Vegas, NV

June 12-14, 2017
New York, NY

December 4-6, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAR321

Auditing Strategic Risks

Adding Value by Validating Critical Initiatives

Seminar Focus and Features

This three-day seminar is designed for auditors who need to understand and identify the significant risks that strategic initiatives bring to the organization. You will learn the key risks and known points of failure in the most prevalent strategic initiatives undertaken by organizations including outsourcing, mergers and acquisitions and new systems design and acquisitions.

You will investigate risks associated with claiming a presence on the internet and technologies such as cloud computing. You will discover how to audit these key risks and how to ensure that they have been properly addressed throughout your strategic undertaking. You will cover the audit strategies that must be employed to assure that your efforts yield the maximum return on the audit investment to your organization. You will leave this high-impact seminar with an inventory of all of the key risks in these critical areas and with an audit strategy to address each risk.

Prerequisite: Risk School (OAR201), Using Risk Assessment to Build Individual Audit Programs (OAR321) 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. **Outsourcing/Third-Party Contracting**
2. **Mergers and Acquisitions**
3. **New Systems Design/ Acquisition**
4. **Embracing New Technology**
5. **Internet Presence**

SCHEDULE

April 19-21, 2017
New York, NY

July 17-19, 2017
Boston, MA

September 11-13, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAR330

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 process. You will learn how to define which aspects need to be audited and how to audit them, gain an understanding of the key qualities that an ERM should possess and discover why they are critical. Explore the integration of controls and business risk and find out how to create an oversight tool that can be owned by operations and that will yield real business returns. You will work through a case study that will allow you to put into use what you learned as you are challenged to determine the most appropriate audit tools, techniques and process for evaluating an ERM situation. You will leave this session with a solid understanding of how a well-structured ERM process should operate, what is critical to its success or failure and how to audit it to determine its efficacy.

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 and Compliance Managers; Internal and External Auditors; Information Technology Auditors; and Operations Managers

What You Will Learn

1. **Defining the Key Components of ERM**
2. **A Top-Down Risk-Based Approach to Establishing an ERM Process**
3. **Integrating Business Risk and Internal Control**
4. **Developing an ERM Audit Process**
5. **Auditing the ERM Process**
6. **Auditing the Effectiveness of ERM in the Organization**
7. **Case Study**

SCHEDULE

October 5-7, 2016
Orlando, FL

December 5-7, 2016
Boston, MA

February 6-8, 2017
San Francisco, CA

May 8-10, 2017
Orlando, FL

August 7-9, 2017
Washington, DC

November 6-8, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAR341

"Excellent presentation. Instructor supported topics and presentation with numerous real-world experiences and examples."

Sean Bartholomew,
Senior Examiner,
FDIC

Risk Management Masterclass

Strategies and Tools for Advanced Risk Management Leadership

Seminar Focus and Features

This three-day course is designed to assist leaders who play a role in or are responsible for risk management at their organization. It is also beneficial for those who want to learn more about risk and enhance their leadership skills in promoting risk management in their organizations. Together, we will explore the history, foundation and evolution of risk and risk management, learn how to assess an organization's risk willingness and appetite, review organizational roles and responsibilities in risk including internal audit and understand what is necessary for successful risk management. We will also discuss the pros and cons of internal controls and the approaches to assess them. Participants will dive into the good, the bad and the ugly of most ERM journeys. We will review our understanding of leadership including soft skills, strategies, approaches and value-based leadership. We will close with the development of a tailored action plan for each participant to use immediately upon completion of the course. Towards the end of this course, participants will review internal control and risk definitions, components and principles, assess the pros and cons of different risk frameworks, analyze ERM fundamentals, essentials, frameworks and tools and discuss the importance of leadership in risk management.

Prerequisite: Auditing the Enterprise Risk Management Process (OAR341) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Executives, Chief Audit Executives, Chief Compliance Officers, Internal Audit and Risk Management Leaders, Risk Directors and Managers, Supervisors, Internal and External Auditors from private, public and not-for-profit sectors

What You Will Learn

1. **The History and Learning's of Risk and Risk Management**
   - how our understanding of risk has evolved
   - process improvements and innovation in risk management
2. **Foundation and Elements of Successful Risk Management**
   - tone at the top
   - review of risk assessment models
   - roles and responsibilities corporate wide
   - corporate governance
   - corporate compliance
   - culture of risk awareness
   - the roles of the executive suite, the audit committee and the board
   - sponsorship–risk champions
   - ERM: how do we define it, promote it and communicate it
   - different compliance functions
   - reviewing the various elements of an ERM system and program
   - integrated risk management
3. **Organizational Risk Willingness and Appetite**
   - how willing is your organization to embrace risk management?
   - how welcoming is your corporate culture to risk?
   - how to take your organization's and stakeholder's risk temperature?
   - can you only go as far as your organization and sponsors are willing to go?
4. **Role of Internal Audit in Risk Management**
   - what role should Internal Audit play in risk?
   - what is the value of internal auditing in regards to risk?
   - risk-based auditing
   - assisting with ERM as an audit department
   - should IA own ERM?
   - IA's role with risk management and risk assessment
   - risk and the audit universe
   - review of different approaches to communicate risk assessment results
   - how can IA help in risk prioritization?
   - what is the process of conducting a risk-based audit?
5. **What is Risk?**
   - how is risk understood at each level of the organization?
   - what are the different kinds of risks and how are they grouped?
   - what risks are required to be analyzed by regulation?
   - understanding risk appetite, risk tolerance, opportunities and threats
   - recognizing risk in change management
6. **Internal Control and Risk**
   - different types of controls and how they help with risk
   - top-down risk-based controls
   - preventive and detective controls
   - key controls
   - is it really a control?
   - do our controls cover the most important risks?
   - control design processes
   - the need to adjust controls along with risks as needed
7. **ERM - the Good, the Bad, the Ugly and the Potential**
   - ERM definition and purpose
   - how to build a business case for ERM
   - implementation challenges with ERM programs
   - risk balance vs. risk overkill
   - risk identification and establishing risk priority ranking
   - how to improve ERM to enhance value
   - agile meets ERM: the importance of flexibility
   - navigating risk management trials
   - converting new risk management disciples
   - tailoring your marketing and communication to address specific needs and stakeholders
   - KISS
   - the basics must be clear and simple
   - IIA standards and essentials
   - assessing and monitoring risks
   - risk identification, assessment, response, monitoring and reporting
   - efficient use of the risk matrix and register
   - taking advantage of low hanging fruit
8. **ERM Fundamentals, Essentials, Frameworks and Tools**
   - models, elements and frameworks of ERM
   - why do we need frameworks and models?
   - how do we implement ERM?
   - how does COSO, ISO, and COBIT impact ERM?
   - what are the elements and changes of COSO ERM?
   - pros and cons of different risk assessment frameworks
   - importance of understanding the external and internal landscape
   - the language of risk
   - levels of risk and examples
   - ERM strategy
   - can ERM be all things to all people?
9. **The Importance of Leadership in Risk Management**
   - leadership–what is it? why is it needed? how does it help?
   - different ways to lead
   - soft skills and strategies
   - power and influence
   - landmines, traps and foxholes
   - trials and tribulations
   - leading with strengths and values

SCHEDULE

November 14-16, 2016
New York, NY

May 1-3, 2017
New York, NY

October 16-18, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAR510

Bank Internal Audit School

Understanding Banking, the Associated Risks and How to Control Them

Seminar Focus and Features

This comprehensive, four-day seminar is designed to provide internal auditors with the critical skills they need to conduct internal audit assignments for financial institutions using internationally recognized best practices. Participants will explore the key areas of banking to ensure that they appreciate the risks inherent in the activities conducted and will then identify the best audit approaches to address these risks. The course is based on the use of the risk-based approach which is designed to ensure that the auditors' work is both effective and efficient. By attending this course, you will obtain a general understanding of the banking industry and internationally recognized best practice approaches to a range of products including, personal and corporate lending, deposit taking, trade finance and treasury instruments. You will work in teams to build sample audit programs which will be provided to participants at the conclusion of the course.

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 and Compliance Managers

What You Will Learn

1. **How to Audit a Bank**
   - planning
   - materiality
   - risk appetite
   - the risk assessment exercise
   - fraud and money laundering deterrence responsibilities
   - relationship to external audit
   - home/host regulation
   - branch and representative office audits
   - introduction to the Basel Accord (2, 3 and 4)
2. **Deposits and Deposit Taking**
   - how banks are funded
   - current accounts
   - deposit accounts
   - retail funding
   - customer identification
   - the customer recording process
   - payments in and out of deposits
   - dormant accounts
   - notice accounts
   - reporting deposits
   - key risk issues within deposits and deposit taking
3. **Funds Transmission and Clearing Services**
   - payment mediums
   - bulk paper clearing
   - cash and debit cards
   - credit cards
   - Internet banking
   - ATM machines
   - SWIFT and international payments
4. **Personal Lending**
   - the customer
   - connected lending
   - overdrafts
   - personal loans
   - mortgage lending
   - retail customer analysis
   - credit scoring
   - using external agencies
   - knowing your customer
   - the drawdown process
   - reporting personal lending
5. **Corporate Lending**
   - the customer
   - connected lending
   - the credit application
   - rating agencies
   - project finance
   - structured lending
   - sovereign debt
   - reporting corporate lending
6. **Security and Provisioning**
   - introduction
   - fixed charges
   - floating charges
   - guarantees
   - mortgages
   - provisioning
7. **Trade Finance and Finance of Trade**
   - trade finance defined
   - bills of exchange
   - promissory notes
   - export credits
   - factoring and forfeiting
   - invoice discounting
8. **Branch Banking**
   - roles conducted at branches
   - nature of audit work to be conducted
   - reviewing branch records
   - human resources issues
   - compliance issues
   - reporting and management
9. **Private Banking**
   - the services of a private banker
   - asset management
   - offshore bank accounts
   - politically exposed persons
   - key risks in personal banking
10. **Investment Banking**
    - long-term finance
    - venture capital
    - debt financing
    - underwriting
    - structured finance
    - due diligence processes
    - documentation and liability
    - income generation
11. **Dealing and the Dealing Room**
    - the difference between the trading book and the banking book
    - the deal process
    - telephone dealing
    - electronic dealing
    - controls and the control environment
    - Basel rules on operational risk
    - compliance/general conduct
12. **Foreign Exchange**
    - calculating foreign exchange rates
    - the foreign exchange market
    - the language of foreign exchange
    - spot rates and cross rates
    - systems of accounting
    - international accounting standards
    - principles of valuation
13. **Forward Contracts**
    - calculating forward foreign exchange rates
    - advantages and disadvantages
    - positions and hedging
    - spot and forward transactions
    - principles of valuation
    - forward rate agreements
    - forward to forward contracts
    - international accounting standards
14. **Futures and the Futures Market**
    - introduction to financial futures
    - futures exchanges
    - types of futures contracts
    - quotation of futures contracts
    - margin accounting
    - confirmation and control
15. **Options and the Options Market**
    - introduction to options
    - types of options contract
    - premiums, margin and exercise
    - option terms and payoffs
    - confirmation and control
16. **Swaps and the Swaps Market**
    - interest rate swaps
    - currency swaps
    - credit derivatives
    - weather derivatives
    - advantages of swap structures
    - pricing a swap
    - credit risk and collateral
    - ISDA documentation
    - hedging and hedge accounting
    - control and confirmation

SCHEDULE

November 7-10, 2016
New York, NY

March 20-23, 2017
New York, NY

June 19-22, 2017
Chicago, IL

July 31-August 3, 2017
Boston, MA

November 13-16, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2895 **32 CPEs**

Web: misti.com/OAP385

OAP380 NEW!

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 been 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

October 5-7, 2016
Chicago, IL

April 3-5, 2017
Boston, MA

July 24-26, 2017
Washington, DC

October 30-November 1, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2495 **24 CPEs**

Web: misti.com/OAP380

OAP382 NEW!

Auditing Debt Collection

Learn to Develop an Audit Program for Optimal Receivables Collection

Seminar Focus and Features

Cashflow is crucial to any business and the receivables audit is therefore a key assignment within any firm. The modern recoveries manager needs to employ the right balance between old-fashioned collection methods and automation if he is to achieve the best returns. Consequently, internal auditors need to appreciate the nature of the techniques that are applied and how they will be assessed.

This two-day course is designed to provide internal auditors with the skills they require for auditing the management and operation of the problem debt assessment and recovery system. Emphasis will be placed on practical and theoretical, with numerous examples and case studies presented throughout the course. In-depth discussions among delegates will be facilitated so that attendees may pool their experiences and learn from both mistakes and successes.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or have equivalent experience. Some knowledge of bank lending and debt recovery systems would be an advantage but is not essential
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. Auditing Debt Governance
2. Auditing Debt Recovery Strategy
3. Standardized or Customized?
4. Standard and Customized Techniques
5. Negotiation Techniques
6. The Court Option

SCHEDULE

October 3-4, 2016
Chicago, IL

April 6-7, 2017
Boston, MA

July 27-28, 2017
Washington, DC

November 2-3, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2095 **16 CPEs**

Web: misti.com/OAP382

Understanding and Auditing Investments and Derivatives

Identifying and Mitigating Risks Specific to Investment and Derivative Strategies

Seminar Focus and Features

Auditing investments and derivatives can be very challenging in today's volatile markets. In this three-day seminar you will gain a basic understanding of investment and derivative terminology, the strategies entered into by portfolio managers/investment managers/traders and the core processes used in the risk management and back-office operations. You will examine front-office, back-office and middle-office activities; control objectives; red flags; and internal control best practices. In addition, you will learn to differentiate between derivative hedging and speculating activity and gain an understanding of the new financial regulation changes being introduced into the market over the next several years. You will pay special attention to identifying the specific risks common to investment and derivative strategies and cover how to minimize those risks with a strong internal control environment. Through class discussions, case studies and practical exercises, you will learn how to develop meaningful audit programs to use in one of the most material areas an auditor can review.

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 and External Auditors; Risk and Compliance Managers and Middle Managers; Investment Auditors and Accountants; Regulators and Bank Supervisors

What You Will Learn

1. **Introduction to Investment and Derivative Auditing**
2. **Understanding the Investment Environment**
3. **Understanding the Derivative Environment**
4. **The Forward and Futures Contracts**
5. **The Option Market**
6. **The Swap Market**
7. **The Investment Infrastructure: Best Practices**
8. **Controlling Investment and Derivative Risks**
9. **Accounting for Derivatives**
10. **Establishing a Comprehensive Compliance Function: The Current State of the New Financial Regulation**
11. **Case Study: Auditing the Investment and Derivative Environment**

SCHEDULE

November 2-4, 2016
Chicago, IL

March 13-15, 2017
Las Vegas, NV

May 8-10, 2017
New York, NY

August 28-30, 2017
Chicago, IL

December 4-6, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2495 **24 CPEs**

Web: misti.com/OAP285

Community Banking Governance and Assurance Practices

Understanding Best Practice Operational Control Issues

Seminar Focus and Features

While there is no specific definition for a "Community Bank," most would agree that it is usually a financial institution with assets up to about $1 billion and with a primary business focus within their local geographic area. This three-day course will provide a realistic look at those financial institutions including these banks, Savings & Loans and Credit Unions and their issues and provide a clear path for understanding good operational control practices issues from all major functions including: Deposit Operations, Lending and Lending Operations, Compliance, IT and Vendor Management. We will provide a basis for success from a control perspective using high performance institutions as an example and identify gaps that are counter-productive to success of organizational strategies.

Prerequisite: None

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

State-Level Banking Associates

What You Will Learn

1. **Current Issues Discussion and Lecture - Banking and Community Banking Specific**
2. **Enterprise Governance**
   - application in smaller institutions
   - organizational structures enabling governance in smaller institutions
   - workable implementation
3. **Regulations and Compliance and Their Impacts**
   - FFIEC - FDIC, OCC, FRB, NCUA, STATE, etc. and their unique differences
   - BSA/AML
   - Dodd/Frank
   - GLBA
   - FFIEC Guidance
4. **High Performance Community Banks**
   - primary controls, policies and procedures for success
5. **Operational Internal Control Practices**
6. **Deposit Operations**
   - internal functions and services
   - Ebanking services
7. **Lending Internal Control Practices**
   - credit risks
   - loan operations
8. **Customer Services Internal Control Practices**
9. **IT Internal Control Practices**
   - value/risk of technology
   - information assets security
   - computer operations (in house processing)
   - network operations

SCHEDULE

February 6-8, 2017
San Francisco, CA

June 7-9, 2017
New York, NY

October 9-11, 2017
Boston, MA

Available In-House (page 8).

Tuition $2495 **24 CPEs**

Web: misti.com/OAP381

OAR385 NEW!

Auditing Basel III and the ICAAP/RRP

Learn the Latest Tools, Techniques and Best Practices for Economic Capital Calculation and Management

Seminar Focus and Features

As banks strive for value creation in a highly competitive environment, they inevitably create risks. The greatest threat to a financial institution is when such risks are not properly identified, measured or managed. In these circumstances the result is invariably unexpected losses, which, as the financial crisis demonstrates, can threaten the very existence of banks of all sizes. The regulatory response to recent events is contained in Basel III which sets out to make capital requirements more risk-sensitive, enhance risk coverage and strengthen the loss absorbency of available capital. It introduces the concept of building capital buffers during good times so that banks are better positioned to absorb the losses that occur during periods of stress.

Basel III further introduces new liquidity management standards. Notwithstanding Basel III, banks continue to focus their risk management programs on Basel II compliance as these new rules are progressively implemented. The ICAAP is provided to the regulators to enable them to understand the uncertainties within the capital calculation. It is required to be audited in most countries prior to being provided to the regulator and therefore represents a high risk audit assignment. This internal audit course will focus on the use of the risk-based approach being applied to these business areas. Delegates will develop audit programs during the course of the training event which will be of benefit to their firms in practice.

Prerequisite: This course is designed for internal auditors with knowledge of internal audit techniques who are seeking to learn about the audits of these areas. Knowledge of internal audit is assumed and some familiarity with banking products would be an advantage.

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

This course is designed for internal audit professionals who will be involved with the audit of Basel II, Basel III and/or the ICAAP. It will also be of interest to others that require knowledge of the risk issues arising.

What You Will Learn

1. **Basel II and Enterprise Risk Management**
2. **Basel II and Operational Risk**
3. **Basel II - Trading Book Issues including Market Risk**
4. **Basel II and Credit Risk**
5. **Basel III**
6. **Basel III - Capital and Its Loss Absorbability**
7. **Stress Testing**
8. **The Internal Capital Adequacy Assessment Process (ICAAP)**
9. **The Recovery and Resolution Plan**

SCHEDULE

December 7-9, 2016
New York, NY

May 8-10, 2017
New York, NY

September 25-27, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2495 **24 CPEs**

Web: misti.com/OAR385

OAP384

Auditing the Credit Department

The Key Control Issues Within the Credit Function and Its Role Within the Business

Seminar Focus and Features

The demands of regulation and business practices have made credit departments within banks increasingly more complex. Since the internal audit function needs to address all areas of a financial institution, including the credit department, auditors face additional challenges.

This interactive, two-day seminar will hold a magnifying glass to the credit function and examine a proven approach for auditing this critical area. You will review public information on current company structures to discover the role of the credit department within a major financial services organization. You will gain an understanding of the risks of lending decisions and cover the difference in audit approaches between the audits of personal and corporate lending. You will also explore personal and corporate credit analysis and get up to speed on the latest regulatory requirements. Class exercises throughout this intensive seminar will reinforce what you learn.

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 Credit Auditors; Audit Directors and Managers; Risk Managers and Audit Committee Members

What You Will Learn

1. **Introduction to Credit Risk**
   - the role of the Credit Committee
   - Credit Committee minutes
2. **Lending**
   - understanding the risks of lending decisions
   - planning the audit
3. **Personal Credit Analysis**
   - credit scoring and the use of external information
   - model and collateral valuation
   - planning the audit of personal credit
4. **Corporate Credit Analysis**
   - balance sheets and financial analysis
   - non-financial analysis
   - the credit report
   - corporate collateral and collateral management
5. **Regulatory Requirements**
   - the implications of the Basel Accord for credit audit
   - the latest tools and techniques to measure, manage and monitor credit risk
   - auditing the loss given default
6. **Model Risk and the Credit Function**
   - sovereign credit ratings
   - credit arrears and arrears reporting

SCHEDULE

December 5-6, 2016
New York, NY

March 16-17, 2017
Las Vegas, NV

May 11-12, 2017
New York, NY

September 28-29, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2095 **16 CPEs**

Web: misti.com/OAP384

OAP241

COSO 2013 Internal Control Integrated Framework

Implementing the Framework to Improve Internal Controls

Seminar Focus and Features

COSO released an updated Integrated Control Framework (IC-IF) in 2013. In this interactive, two-day seminar you will learn how this principles-based approach can be designed effectively and deployed successfully within organizations. Participants will also examine the implications for business leaders, process owners and internal auditors, who can use the framework to add value while providing audit and consulting services.

During this course, participants will review the differences between the 1992 and the updated 2013 models, the implications on the system of internal controls and acquire the tools necessary to effectively design, implement and evaluate their organization's system of internal controls. You will leave with the skills necessary to perform an assessment of your organization, and know how to apply the seventeen principles representing the fundamental concepts associated with the components of the framework.

Prerequisite: Fundamentals of Internal Auditing (OAG101) or equivalent experience and familiarity with the 1992 COSO Internal Control Framework

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Senior Auditors, Internal and External Auditors, Audit Managers and Directors

What You Will Learn

1. Understanding COSO
2. COSO Implementation and Evaluation Tools
3. Objectives
4. Control Environment
5. Risk Assessment
6. Control Activities
7. Information and Communication
8. Monitoring
9. Conclusion

SCHEDULE

September 22-23, 2016
Chicago, IL

December 15-16, 2016
Orlando, FL

February 9-10, 2017
San Francisco, CA

May 18-19, 2017
Washington, DC

December 7-8, 2017
Orlando, FL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/OAP241

"I got the information I needed. The course moved at a good pace and had good interaction with all participants."

Kirstin Carlson,
Project Manager,
Provaliant

OAP352

Governance, Risk and Compliance

Real-World Solutions for Creating a Best-Practice GRC Framework

Seminar Focus and Features

In this three-day, interactive seminar you will learn from a practicing CRO/CCO how to implement a best-in-class GRC Integrated Framework in your organization. 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. You will also learn the steps to take to make the internal audit function a strategic part of the GRC framework. You will be provided with the tools and best practices you need to implement an integrated GRC model in your organization. You will leave this seminar with a specific action plan and a "snapshot" of what an integrated governance framework will look like in your organization.

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

Who Should Attend

Chief Compliance Officers, Chief Audit Executives, Audit Directors & Managers; Chief Risk Officers & Chief Ethics Officers; Internal & External Auditors; those newly charged with GRC responsibilities

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"

What You Will Learn

1. GRC: First, Answering the Important Questions
2. Understanding Governance Risks: The GRC Model
3. A Strategic Look: Expectations and Challenges in Building and Implementing the GRC Framework and Model
4. Analyzing the Tone-at-the Top and Tone-in-the-Middle
5. Four Key Components and Your Roadmap to Success
6. GRC Focus on Managing Risks
7. Compliance and Regulatory Matters: The Core Strategy
8. Ethics: Values and Behavior
9. Investigations and Fraud Reporting
10. Key Strategy: Implementing the Chief Risk Office/Chief Compliance Office

SCHEDULE

October 17-19, 2016
New York, NY

March 13-15, 2017
New York, NY

May 22-24, 2017
Anaheim, CA

October 16-18, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/OAP352

ITP241

COBIT® 5: Integrating COBIT into Your IT Audit Process

Utilizing COBIT 5 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 5 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 5 that can be utilized in executing IT audits. You will also discover how to use COBIT 5 in conjunction with other internationally recognized standards and frameworks.

During the seminar you will explore examples using COBIT 5 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 5 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

IT Auditors, Managers and Directors; QA personnel; Information Security Managers, Auditors, Directors and Analysts; CIOs

What You Will Learn

1. COBIT Background
2. Summary of COBIT 5
3. International Security Standards, Frameworks
4. Assessing IT Governance Using COBIT 5
5. Risk Management
6. Security Management
7. Manage Continuity
8. Integrating the COBIT 5 Process Capability Model
9. Performing an Assessment Using COBIT 5.9
10. COBIT Related Resources

SCHEDULE

May 8-10, 2017
San Francisco, CA

October 23-25, 2017
New York, NY

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ITP241

ITP262

Testing IT General Computer Controls for Sarbanes-Oxley

A Road Map for Identifying, Testing, Documenting and Remediating Common SOX General Computer Controls

Seminar Focus and Features

During this two-day seminar you will gain a solid understanding of the entire methodology for reviewing and testing general computer controls in a Sarbanes-Oxley environment. You will cover documenting the GCC environment, identifying, developing and executing test plans, identifying control gaps, developing remediation plans, communicating and reporting testing results. You will the explore the 12 areas of GCC identified by the Information Technology Governance Institute (ITGI) and generally recognized by the PCAOB and external audit firms as critical for testing GCCs and examine the underlying practical details of how those areas of GCC relate to IT environments. You will look at compiling real-world GCC testing procedures, identifying key control processes from example GCC narratives and pinpointing control design gaps. You will develop efficient test plans utilizing automated tools while determining appropriate timelines, review elements of workpaper documentation from a SOX perspective and use classroom exercises to walk through documenting and testing key controls from selected components in the 12 GCC areas. We will identify control implementation gaps and create risk ranking criteria, potential remediation plans, compensating controls, testing procedures and communication strategies to pursue with your external auditors. We will review lessons learned and cover best practice control techniques you can implement and test as part of your compliance program.

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

IT Auditors, Managers and Directors; QA personnel; Information Security Managers and Analysts; External Auditors

What You Will Learn

1. SOX GCC Requirements as Defined by ITGI
2. IT SOX Testing Methodology
3. GCC Documentation
4. GCC Testing
5. GCC Remediation
6. Automated Testing Techniques and Tools
7. IT Recommended Practices for SOX and Other Compliance Initiatives

SCHEDULE

January 30-31, 2017
San Francisco, CA

May 11-12, 2017
Boston, MA

September 14-15, 2017
Chicago, IL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ITP262

IT Auditing and Controls

AVAILABLE ONLINE

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 intensive, 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.

NOTE: This seminar covers topics found in Chapters 1, 4 and 5 of the CISA® Review Manual.

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

TOP 10 IN-HOUSE

Who Should Attend

Financial, Operational, Business Applications, Internal and External Auditors who want an introduction to IT auditing

What You Will Learn

1. **Introduction to IT Risks and Controls**
   - role of IT
   - risk definitions
   - risk assessment
   - information security objectives
   - IT controls cost/risk balance
   - internal control overview
   - accountability and auditability
   - integrated auditing
2. **Planning IT Audits**
   - definition of internal audit
   - IT audit planning
   - audit universe/IT audit universe
   - risk criteria
   - audit engagement planning
   - IT control categories
   - mapping risk and control categories
3. **Audit and Control Frameworks and Standards**
   - maintaining objectivity
   - what is a standard?
   - COSO
   - GAO Green Book
   - IIA Global Technology Audit Guides
   - COBIT®
   - ISO 27002 Security Standard
4. **Basics of Information Technology**
   - computer hardware
   - Central Processing Unit/ Memory
   - Operating Systems (OS)
   - mainframe
   - client/server technology
   - virtualization/virtual servers
   - batch and interactive models
5. **Database Technology and Controls**
   - managing information
   - database terminology
   - Database Management Systems (DBMS)
   - hierarchical databases
   - relational databases
   - database risks
   - database audits
6. **Network Technology and Controls**
   - networking risks
   - what is a "network"?
   - OSI Model
   - Local Area Networks (LANs)
   - Wide Area Networks (WANs)
   - network devices
   - firewalls
   - intrusion detection systems (IDS/IPS)
   - Virtual Private Networks (VPNs)
   - wireless
   - the Internet
   - cloud computing
7. **IT Governance**
   - audit's role in IT governance
   - IIA professional practices framework - governance
   - linking business and IT strategies
   - IT Governance Objectives
   - COBIT® 5 – IT governance/ management
   - IIA GTAG – auditing IT governance
   - separation of duties
   - assessing outsourced IT functions
8. **IT General Controls**
   - logical security
   - change management
   - business continuity/disaster recovery
   - operation controls
   - physical security
   - environmental exposures
   - system development
9. **Business Application Controls**
   - business application control categories
   - business application risks
   - what is a transaction?
   - transaction life cycle
   - business application audit objectives
   - business application controls
   - the future of applications

SCHEDULE

September 19-21, 2016
Chicago, IL
October 4-6, 2016
Dallas, TX
October 31-November 2, 2016
San Francisco, CA
December 5-7, 2016
Miami, FL
February 6-8, 2017
San Francisco, CA
March 27-29, 2017
Denver, CO
April 24-26, 2017
Boston, MA
May 1-3, 2017
Chicago, IL
June 5-7, 2017
San Diego, CA
July 17-19, 2017
Boston, MA
August 7-9, 2017
Washington, DC
September 18-20, 2017
Orlando, FL
October 11-13, 2017
Chicago, IL
November 6-8, 2017
Anaheim, CA
December 4-6, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ITG101

"Informative and a perfect class for those who are new to IT and IT Audit."

Nick Mayer,
Associate IT Auditor,
American Financial Group

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

Who Should Attend

IT, Financial, Operations and Business Applications Auditors; Audit Managers who require an understanding of application controls and audit approaches for business application systems

What You Will Learn

1. **Introduction to Business Application Systems**
   - types of business applications
   - objectives of an application audit
   - application control ownership
   - integrated auditing
   - data vs. information
2. **Business Application Transactions**
   - transaction-based application auditing
   - application risk assessment factors
   - establishing audit priorities
3. **Top-Down Risk-Based Planning**
   - planning the business application audit
   - defining the business environment
   - determining the application technical environment
   - performing a business information risk assessment
   - identifying key transactions
   - developing a key transaction process flow
   - evaluating and testing application controls
4. **Application Controls**
   - business application audit objectives
   - application transaction life cycle
   - transaction origination
   - completeness and accuracy of input, processing, output
   - output retention and disposal
   - user review, balancing, reconciliation
5. **Testing Application Controls**
   - testing automated and manual controls
   - testing alternatives
   - sample size
   - negative assurance testing
   - types of audit evidence
   - CAATs and data analysis
6. **Documenting Application Controls**
   - evaluating and documenting internal controls
   - internal control questionnaires
   - narratives
   - flowcharts/process flows
   - risk/control matrix
7. **End-User Computing**
   - end user computing risks
   - practical steps for evaluating spreadsheet controls
8. **Auditing System Development Projects**
   - identifying business risks
   - audit's primary objectives
   - traditional system development life cycle
   - rapid application development
   - managing audit involvement

SCHEDULE

November 3-4, 2016
San Francisco, CA

May 4-5, 2017
Chicago, IL

September 21-22, 2017
Orlando, FL

December 7-8, 2017
Orlando, FL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ITG103

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 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. 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.

NOTE: This seminar covers topics found in Chapters 1, 2, 3, 4 and 5 of the CISA® Review Manual.

Prerequisite: None

Advance Preparation: None

Learning Level: Basic

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Financial, Operational, Business Applications, other Internal and External Auditors; and compliance personnel who want an introduction to IT auditing

What You Will Learn

1. **Introduction to IT Risks and Controls**
   - risk assessment
   - information security objectives
   - IT controls cost/risk balance
   - accountability and auditability
   - integrated auditing
2. **Planning IT Audits**
   - risk criteria
   - audit engagement planning
   - IT control categories
   - mapping risk and control categories
3. **Audit and Control Frameworks and Standards**
   - maintaining objectivity
   - what is a Standard?
   - COSO
   - GAO Green Book
   - IIA Global Technology Audit Guides
   - COBIT®
   - ISO 27002 Security Standard
4. **Basics of Information Technology**
   - computer hardware
   - central processing unit/memory
   - Operating Systems (OS)
   - mainframe
   - client/server technology
   - virtualization/virtual servers
   - batch and interactive models
5. **Database Technology and Controls**
   - managing information
   - Database Management Systems (DBMS)
   - hierarchical databases
   - relational databases
   - database risks
   - database audits
6. **Network Technology and Controls**
   - what is a "network"?
   - OSI Model
   - Local Area Networks (LANs)
   - Wide Area Networks (WANs)
   - network devices
   - firewalls
   - Intrusion Detection Systems (IDS/IPS)
   - Virtual Private Networks (VPNs)
   - wireless
   - the Internet
   - cloud computing
7. **IT Governance**
   - audit's role in IT governance
   - IIA Professional Practices Framework–Governance
   - linking business and IT strategies
   - IT governance objectives
   - COBIT® 5–IT Governance/Management
   - IIA GTAG–Auditing IT Governance
   - separation of duties
   - assessing outsourced IT functions
8. **IT General Controls**
   - logical security
   - change management
   - business continuity/disaster recovery
   - operation controls
   - physical security
   - environmental exposures
   - system development
9. **Business Application Transactions**
   - what is a transaction?
   - transaction-based application auditing
   - application risk assessment factors
   - establishing audit priorities
10. **Top-Down Risk-Based Planning**
    - planning the application audit
    - 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
11. **Data Input and Processing Models**
    - model comparison
    - batch input–batch processing
    - on-line input–batch processing
    - real-time input/real-time processing
12. **Business Application Controls**
    - business application transaction life cycle
    - transaction origination
    - completeness and accuracy of input, processing and output
    - output retention and disposal
    - data file controls
    - user review, balancing, reconciliation
    - end-user documentation
13. **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
14. **Documenting Business Application Controls**
    - evaluating and documenting internal controls
    - Internal Control Questionnaires (ICQ)
    - flowcharts/process flows
    - control matrix
15. **End User Computing**
    - change control risks
    - purchased application risks
    - spreadsheets–typical errors/risk factors
    - practical steps for evaluating spreadsheet controls

SCHEDULE

September 12-15, 2016
San Diego, CA

October 17-20, 2016
New York, NY

November 7-10, 2016
Las Vegas, NV

December 12-15, 2016
Orlando, FL

February 27-March 2, 2017
Atlanta, GA

March 13-16, 2017
Las Vegas, NV

April 18-21, 2017
Chicago, IL

May 15-18, 2017
Washington, DC

June 12-15, 2017
New York, NY

July 24-27, 2017
Denver, CO

August 21-24, 2017
Anaheim, CA

September 25-28, 2017
Chicago, IL

October 23-26, 2017
New York, NY

November 13-16, 2017
Boston, MA

December 18-21, 2017
San Diego, CA

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/ITG121

Intermediate IT Audit School

A Risk and Compliance Approach to Auditing the IT Environment

Seminar Focus and Features

A week no longer passes that does not include more headline-grabbing news of a large "cyberattack" or "cyberbreach". These hacker threats, evolving technologies and staff shortages challenge IT auditors to address the enterprise's increasing IT risks. The common thread through these security incidents is the requirement for information security, individual privacy and effective controls at all levels of the enterprise. 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. You will apply COBIT® and ISO-27002 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. Each topic will be accompanied with detailed discussions representing IT control best practices.

NOTE: This seminar covers topics found in all the chapters in the CISA® Review Manual, and is continually updated to keep pace with evolving technologies, trends and techniques.

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 Applications, IT and External Auditors; QA personnel; Audit Managers and Directors; Information Security Managers and Analysts

What You Will Learn

1. **Risk Assessment and Audit Planning**
   - IT threats, risks and exposures
   - IT infrastructure risks
   - information classification
   - building the IT audit universe
   - establishing risk criteria
2. **Compliance Management: Regulations, Standards and Frameworks**
   - eDiscovery
   - COSO and GAO Green Book
   - ISO 27001, ISO 27002 Security Standards
   - COBIT® 5
   - IIA Global Technology Audit Guides (GTAGs)
   - Center for Internet Security–Critical Security Controls (CIS CSC)
   - Federal Information Security Management Act (FISMA)
   - DOD Checklists/STIGs
   - ITIL
   - European Union–Data Protection Directive
   - Open Web Application Security Project (OWASP)
   - Payment Card Industry–Data Security Standard (PCI DSS)
3. **IT Governance**
   - IT governance risks and responsibilities
   - IT governance components
   - information security governance
   - separation of duties
4. **User Access Controls**
   - common access control issues
   - social media and social engineering
   - user identification and authentication
   - log management
   - privileged access monitoring
   - distributed web applications
   - mobile computing
5. **Encryption Demystified**
   - encryption concepts and key management
   - symmetric/asymmetric encryption
   - digital signatures
   - Public Key Infrastructure (PKI)
   - Certificate Authorities (CAs)
   - encryption key management audit steps
6. **Network Perimeter Security**
   - network terminology and risk analysis
   - OSI network protocol model
   - threat and vulnerability management
   - firewalls
   - Intrusion Detection Systems (IDS/IPS)
   - Virtual Private Networks (VPNs)
   - wireless
   - cloud computing
7. **Operating System Software**
   - virtualization and hypervisors
   - patch management
   - privileged administrative access
   - vulnerability assessments (health checks)
   - log management
8. **Database Management Systems (DBMS)**
   - relational databases
   - Structured Query Language (SQL)
   - DBMS risks and controls
9. **System Development and Change Management**
   - system development business risks
   - audit's primary objectives on systems development projects
   - assessing project management
   - audit as a value added service
   - configuration and change management
   - web application development risks and controls
   - end user computing risks and controls
10. **Business Continuity and Disaster Recovery Planning**
    - Business Impact Analysis (BIA)
    - Recovery Point Objectives (RPO)
    - Recovery Time Objectives (RTO)
    - application recovery priority
    - continuity plans and procedures
11. **Auditing Outsourced IT Operations**
    - outsourcing risks
    - ensuring strong contractual agreements
    - right to audit
    - SSAE-16, SOC1, SOC2, SOC3 reports
    - relationship monitoring
    - audit focus areas
12. **Executing IT Audits**
    - IT audit planning
    - testing IT controls
    - integrated auditing

SCHEDULE

September 26-29, 2016	San Francisco, CA
October 17-20, 2016	**New York, NY**
November 14-17, 2016	Las Vegas, NV
December 12-15, 2016	**Orlando, FL**
February 13-16, 2017	Tampa, FL
March 13-16, 2017	**Las Vegas, NV**
April 18-21, 2017	Atlanta, GA
May 15-18, 2017	**Washington, DC**
June 12-15, 2017	**New York, NY**
July 10-13, 2017	Chicago, IL
August 21-24, 2017	**Anaheim, CA**
September 11-14, 2017	Denver, CO
October 23-26, 2017	**New York, NY**
November 14-17, 2017	Chicago, IL
December 4-7, 2017	Orlando, FL

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/ITG241

ITG341

Advanced IT Audit School

Comprehensive Deep-Dive of IT Audit and Information Security

Seminar Focus and Features

In this information-packed four-day seminar, we will cover, in depth, key building blocks of modern IT audit, physical and logical security, including identity & access management and access control models. We will pay particular attention to the threats and vulnerabilities to web-based e-commerce. 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 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 review safeguard concepts and best practices for secure mobile and wireless applications. We will also discuss standards associated with privacy issues and intellectual property concerns.

Prerequisite: Intermediate IT Audit School (ITG241), 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 Auditors (Internal or External), IT Audit Managers, Information Security Managers and Analysts, IT Managers

What You Will Learn

1. Identity and Access Control Management (I&ACM) Architecture
2. Laws and Standards Affecting IT Audit
3. Web Application Architectures
4. Auditing Web (HTTP) Servers
5. Business Application Software Development and Audit
6. Auditing Application (Middleware) Servers
7. Auditing Database Management Systems
8. Web Services and Service-Oriented Architectures
9. Auditing Remote Access and Mobile Applications

SCHEDULE

September 19-22, 2016
Chicago, IL

November 7-10, 2016
New York, NY

April 24-27, 2017
Boston, MA

June 5-8, 2017
San Diego, CA

August 7-10, 2017
Washington, DC

November 27-30, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/ITG341

ITG213 **NEW!**

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, 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 heightened 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

Financial Auditors, IT Auditors, Application Systems Development Team Leaders, Scrum Masters, Project Sponsors

What You Will Learn

1. What Exactly ARE Agile and Scrum?
2. How to Learn about the Project in Time to Get Involved
3. What Is the Definition 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
10. Testing. Yes, TESTING!
11. DON'T Trust the Interfaces
12. Change Management
13. Reporting Deficiencies

SCHEDULE

April 27-28, 2017
Boston, MA

July 20-21, 2017
Boston, MA

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ITG213

"An intense crash course of IT information, I will use the course materials for years to come."

Paige Sundquist,
Associate IT Auditor,
Fedex

ITG212

Auditing Application Systems Development

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

Seminar Focus and Features

In this three-day seminar you will explore proven audit strategies that will enable you to efficiently audit and evaluate applications systems development in a variety of technical environments. You will review common applications development risks, how to overcome them and what you must do to meet the internal control and documentation requirements of SOX. You will drill down to the unique risks associated with purchased, in-house and web-based applications and learn what you can do to minimize them. You will cover RAD, implementation and control change, design specifications, testing, project management and application software inventory control. You will receive audit programs, questionnaires and sample audit findings you can put to use immediately.

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 Applications, IT and External Auditors; QA personnel; Audit Managers and Directors; and System Analysts

What You Will Learn

1. Technical Environments and Their Impact on Applications Systems Development (ASD)
2. ASD Risks and Auditor Responses
3. The Impact of SOX on ASD
4. Challenges with ASD Methodologies
5. Implementing New Releases of Purchased Application Systems
6. In-House ASD
7. Web-Based ASD
8. Rapid Application Development (RAD)
9. Auditing Application Systems Design Specifications
10. Auditing Internal Controls
11. Auditing Programing, Implementation and Change Control and Complete Security
12. Application Software Inventory Control
13. Auditing Project Management
14. Faster ASD Audits
15. RAD: What to Do About It
16. Reporting Audit Findings and Planning for the Future
17. Automated Audit Tools
18. Applications Development and IT General Controls in a SOX World

SCHEDULE

September 19-21, 2016
Chicago, IL

February 6-8, 2017
San Francisco, CA

May 15-17, 2017
Washington, DC

October 16-18, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ITG212

ITG231

Preparing for the CISA® Examination

An Intensive Review of the Topics Covered in the Certified Information Systems Auditor™ Exam

Seminar Focus and Features

In this four-day seminar, we will focus on everything you need to know to pass the CISA exam. You will cover the essential CISA content areas, including IS audit process, IT governance, systems and infrastructure life cycle management, IT service delivery and support, information asset protection, business continuity and disaster recovery. You will work through sample exam questions and review the correct answers for a better understanding of what the ISACA Certification Board expects.

This intensive prep course is an ideal way to prepare for the exam. You will gain valuable experience answering sample exam questions while strengthening the skills you need to approach accreditation with confidence.

NOTE: *Seminar materials are continually updated to reflect current CISA requirements.*

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

IT, Financial, Operational and External Auditors who are taking or considering taking the CISA examination; anyone seeking an overall understanding of essential IT risks and controls

BONUS

You will receive a copy of the *CISA Review Questions and Answers Supplement*.

What You Will Learn

1. Process of Auditing Information Systems
2. Governance and Management of IT
3. Systems Life Cycle Management
4. Business Application Controls
5. IS Operations and Hardware/ Software
6. Protection of Information Assets
7. Network Infrastructure
8. Network Infrastructure Security
9. Encryption
10. Business Continuity and Disaster Recovery

SCHEDULE

May 1-4, 2017
Chicago, IL

August 14-17, 2017
Boston, MA

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/ITG231

ITP361

A Risk-Based Guide to IT Infrastructure Controls

Focusing on Risk to Improve the Efficiency and Effectiveness of Your IT Audits

Seminar Focus and Features

IT risks are increasingly recognized as critical factors in enterprise risk management. From preventing failures in regulatory compliance to helping avoid devastating harm to the reputation of the organization from headline-making security breaches, IT auditors have an obligation and value-adding opportunities to assess enterprise vulnerabilities through both risk- and enterprise objective-based IT audit planning.

In this three-day seminar you will explore the varied aspects of developing an effective IT audit plan, and examine the use of control standards and frameworks, including COSO ERM. You will review such risk elements in IT audit planning as IT governance risks, business information risks and IT infrastructure risks. You will also cover the increased risks introduced by outsourced IT operations and functions. Throughout this high-impact seminar you will focus on developing an IT audit universe based on assessing enterprise information risks. You will leave this intensive seminar with a proactive strategy that will help you establish a comprehensive enterprise IT audit plan that will boost the efficiency and effectiveness of your IT audits.

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

IT Auditors; IT Audit Managers, Supervisors and Directors; Information Security Managers, Analysts and Directors; Consultants; Risk Managers and Officers

What You Will Learn

1. Risk Management
2. Developing an IT Risk Assessment Framework
3. COSO Enterprise Risk Management
4. Using Risk-Based IT Standards and Frameworks
5. Managing IT Governance Risks
6. Information Security Risk Management
7. System Software and Database Risks
8. System Development and Change Management Risks
9. Disaster Recovery Risks
10. Network Perimeter Security Risks
11. Physical Security and Environmental Risks
12. Outsourced IT: Identifying the Risks

SCHEDULE

October 4-6, 2016
Washington, DC

April 24-26, 2017
Boston, MA

August 7-9, 2017
Washington, DC

October 9-11, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ITP361

ITP265

Integrating Emerging Technology Threats in Your Annual Risk Assessment

Identifying Key IT Risks for Your Organization

Seminar Focus and Features

In this three-day seminar you will learn about the latest vulnerabilities and controls and how to incorporate emerging technology into the annual audit risk assessment process. You will begin with an overview of the annual risk assessment process and its deliverables. After the overview the seminar will specifically focus on various emerging technologies, discussing the vulnerabilities associated with each as well as a few of the possible controls that could reduce the likelihood and impact should the vulnerability be exploited.

There will be a series of class and group exercises so participants may discuss various technologies in order to reinforce the annual risk assessment process and aid in the evaluation of the impact of these new technologies and regulations.

You will take away a general understanding of these newer topics and how to assess and use them to protect your organization. The exercises will help you focus on how to consider developing a risk assessment and possible mitigation strategy for various technologies currently deployed in your organization, or that may be in the near-term.

Prerequisite: Risk School (OAR201), Auditing Strategic Risks (OAR330) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Internal and External Auditors; Audit Managers, Directors and Executives; IT Auditors, Managers and Directors; IT Security Analysts, Managers, Directors and Executives; IT Risk Analysts, Managers, Directors and Executives; Compliance Analysts, Managers, Directors and Executives, CIO's and Consultants

What You Will Learn

1. Risk Management 101 Review
2. IT Governance Committee Trends
3. Regulatory Changes
4. Data Privacy
5. Cybersecurity
6. Mobile Wallet
7. Mobile Banking and POS Technology
8. Web Applications/Web Security
9. Consumerization of IT
10. BYOD
11. Cloud Computing - Public to Private
12. Big Data
13. Social Media
14. Wireless

SCHEDULE

October 24-26, 2016
Miami, FL

March 13-15, 2017
Las Vegas, NV

May 8-10, 2017
New York, NY

September 6-8, 2017
San Francisco, CA

November 8-10, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ITP265

ISG101

Introduction to Information Security

A Guide for Anyone Needing Basic Knowledge in Information Security

Seminar Focus and Features

Information security is now an issue for the entire enterprise, not just for security and IT teams. Heightened attention to corporate governance, increasing reports of targeted attacks, more legislation and regulation, data leakage, BYOD, cloud and other cyber security problems are in the media daily, and reports of companies battling the fall-out from breaches have enterprise executives focused on better protecting the business and its assets. But information security can be a minefield of potential disasters waiting to happen if not managed correctly and expertly, or if it's misaligned with business goals.

This intensive three-day training course is filled with tools, techniques, advice and proven strategies geared towards non-technical business professionals for improving the security posture of an organization. During this seminar you, a non-IT security professional, will learn how to respond to the increased emphasis on information security. Attendees will gain an understanding of how to organize and oversee a risk-based enterprise information security program, 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 based around the ISO27000 series and COBIT and take away sample security policies, security review checklists, a glossary of computing terminology and more.

Prerequisite: None

Advance Preparation: None

Learning Level: Basic

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Professionals across all businesses and sectors who need to know more about Information Security; Financial, Operational, Business Application Internal and External Auditors and Risk Managers

What You Will Learn

1. A Definition of the Information Security Environment
2. Security Management: Strategic Components
3. Criteria for Secure Business Applications
4. Protecting the Network Perimeter: Network and Workstation Security
5. Business Continuity Planning (BCP)

SCHEDULE

December 12-14, 2016
Orlando, FL

March 13-15, 2017
Las Vegas, NV

June 5-7, 2017
San Diego, CA

August 7-9, 2017
Washington, DC

December 4-6, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ISG101

ISG103 **NEW!**

Practical Security Assessments

HANDS-ON

Learn to Integrate Your Security Assessments within Development, Business, and Technical Processes and Systems

Seminar Focus and Features

In today's complex security landscape, it is not enough for Infosec teams to set firewall rules and IDSs and hope for the best. Organizations need to have a clear understanding of their threat landscape, what data and systems they're protecting, where the data resides, which assets are most valuable, and how to fine tune defensive controls as the threats and the company's focus change. To make this all happen, security professionals must continually test and assess their network and applications through a combination of manual and automated techniques to ensure controls are working properly and delivering actionable alerts. The old adage, "You cannot manage what you do not measure" is truer now than ever.

In this two-day class, attendees will learn and practice hands-on, real-world assessment techniques. From working with vulnerability scanners to ensuring compliance to industry standards, attendees will explore the techniques and procedures followed by effective security professionals. Some of the highlights will include learning how to weed out false positives and catch false negatives, mapping the network and assets, using the map to identify system vulnerabilities and testing authorizations and permissions. At the completion of this course, security professionals will be able to ensure a comprehensive, ongoing security assessment practice for their organizations.

Prerequisite: None

Advance Preparation: None

Learning Level: Basic

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Information security professionals of all levels, IT auditors with knowledge of cybersecurity

What You Will Learn

1. Introduction
2. Testing Methodology Overview
3. Test Lab and Class Targets
4. Preparation
5. Network Assessments
6. Testing Systems and Services
7. Evaluating Assessments Results
8. Application Assessments
9. Student Real-World Scavenger Hunt Challenge

SCHEDULE

September 26-27, 2016
Orlando, FL

December 5-6, 2016
San Francisco, CA

April 27-28, 2017
Orlando, FL

November 16-17, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2195 **16 CPEs**

Web: misti.com/ISG103

ISG120 NEW!

Tools to Identify and Mitigate Security and Privacy Risks

Protecting the Organization from Cyber-Risks

Seminar Focus and Features

In today's business climate, information risk management has become a top priority at most organizations. International legislation and the best security practices point to information risk analysis as the cornerstone of any program designed to safeguard information assets. In this three-day seminar, attendees will focus on using four tools: Risk Analysis, Business Impact Analysis (BIA), Privacy Impact Assessment and Gap Analysis. These tools are time-tested methodologies for measuring the level of security and privacy risks, and prioritizing information risk reduction approaches in your organization. In this course you will explore the fundamentals of each tool, use them to build models to fit your individual organization's business needs and discover how they can help you determine if you are meeting the security criteria set forth in HIPAA, HITECH, GLBA, Privacy Legislation, Dodd Frank and Sarbanes-Oxley.

At the end of this intensive seminar you will build action plans and learn how to put them into practice in real-world scenarios. You will also develop a process to benchmark your present security posture and use Gap Analysis to improve the security posture of your present environment.

Prerequisite: None

Advance Preparation: None

Learning Level: Basic

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Professionals across all businesses and sectors who need to know more about information security, including financial, operational, business application, and risk managers, and internal and external auditors

What You Will Learn

1. Information Risk Management
2. Information Risk Analysis
3. Developing an Action Plan You Can Implement and Build Upon
4. Follow-Up
5. Business Impact Analysis–Two Tools (BIA for Data Centers, BIA for Business Unit)
6. Developing a BIA Action Plan (Data Centers and Business Units)
7. Using the Business Impact Analysis

SCHEDULE

November 28-30, 2016
San Francisco, CA

February 8-10, 2017
San Francisco, CA

June 12-14, 2017
New York, NY

July 17-19, 2017
Boston, MA

December 4-6, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ISG120

ISG231

Data Privacy: Protecting Your Organization, Customers and Employees

Safeguarding Personal Information in Any Form

Seminar Focus and Features

This three-day course will help attendees understand the myriad and ever-changing data privacy laws and regulations, both U.S.-based and international. We will look at state-by-state comparisons, the role State Attorney Generals play in privacy protection and touch on which industries and countries have particular rules that must be adhered to. This seminar will focus on controls, not theory. The instructor will identify the many controls – some that may be present, others that are new – that will allow attendees to meet privacy objectives. You will discover how less popular processes, such as a privacy impact assessments, can be leveraged alongside more traditional processes like risk analysis, employee awareness and data encryption to obtain proper due care and due diligence. You will explore identity management, data surveillance and other forms of monitoring as a way to ensure data privacy.

Prerequisite: Fundamentals of Information Security (ISG101) or have equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Information Security Managers and Practitioners; Data Privacy Officers or Administrators; Data Security Specialists and Security Administrators; Application Programmers and Test Analysts; IT Auditors, Audit Managers and External Auditors

What You Will Learn

1. Definitions
2. Legal Requirements
3. Privacy and Information Security Strategies and Objectives
4. Privacy Strategy Tools
5. Tools to Achieve Legal and Regulatory Compliance
6. Privacy and Data Outside the Security Perimeter
7. Data Anonymity and Obfuscation
8. Identity Theft
9. Future Issues in Data Privacy and Identity Theft

SCHEDULE

March 20-22, 2017
Las Vegas, NV

April 24-26, 2017
Boston, MA

August 21-23, 2017
New York, NY

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ISG231

ASG203

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.

NOTE: This seminar covers the topics found in Chapters 4 and 5 of the CISA® Review Manual.

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

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Information Security Managers and Analysts; Security Administrators; Information Technology Managers, Planners and Strategists; IT Auditors and Managers; Consultants

What You Will Learn

1. Defining the Distributed Information Technology Environment
2. Developing a Reference Framework for Network Security and Audit: Network Standards and Protocols
3. Demystifying Network Media Access Technologies: Local Area Networks (LANs) and Wide Area Networks (WANs)
4. Network Interconnection Devices: Functionality, Management and Security
5. Enterprise Network Directory Services Security and Audit
6. Keeping a Lid on Network Host Services Security
7. Circling the Wagons: Network Perimeter Security
8. Wrap-Up: Performing a Network Security Risk Analysis

SCHEDULE

October 17-19, 2016
New York, NY

December 12-14, 2016
Orlando, FL

February 6-8, 2017
San Francisco, CA

May 15-17, 2017
Washington, DC

July 17-19, 2017
Boston, MA

August 21-23, 2017
Anaheim, CA

October 23-25, 2017
New York, NY

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ASG203

ISG291

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 ISC² Common Body of Knowledge (CBK) in conjunction with evaluating methods and tools required to construct or audit a comprehensive information security framework. Attendees 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.

To reinforce what you learn in the course and to aid anyone preparing for prominent information security certification examinations, attendees will be provided with unit and course review exercises. Come prepared for five days of intensive learning and return to your office with the foundation of knowledge and know-how needed to take the CISSP exam (or similar), but even more importantly, to help guide your organization as it develops or revises its information security program.

The MISTI instructors for this class have worked closely with one or more of the information security certification organizations (such as (ISC)²).

Prerequisite: None

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Information Security and IT Managers; Information Security Analysts, Security Architects, Security Administrators; System Administrators, Network Administrators, IT Auditors; Consultants; Compliance Managers; and anyone needing a "crash course" in information security concepts and practices

What You Will Learn

1. Security and Risk Management
2. Laws and Standards Affecting Information Security and IT Audit
3. Security Engineering and Security Assessment and Testing
4. Network Security
5. Cryptography
6. Identity and Access Management
7. Software Development Security
8. Asset Security
9. Security Operations Including Availability, Backup, Recovery and Business Continuity Planning

SCHEDULE

September 19-23, 2016
Chicago, IL

December 5-9, 2016
Anaheim, CA

April 3-7, 2017
Boston, MA

June 12-16, 2017
New York, NY

September 25-29, 2017
Chicago, IL

November 27-December 1, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2895 **40 CPEs**

Web: misti.com/ISG291

Introduction to Incident Response

Learning How Breach Preparation Can Drive Down Loss

Seminar Focus and Features

Almost half of the IT security professionals participating in a Ponemon Study stated that they don't have adequate intelligence to detect and investigate incidents and over sixty percent indicate that they cannot stop the exfiltration of sensitive data from their organization. The ability to quickly respond and recover from these incidents is a key factor in minimizing the damage (business and reputation) and containing the costs to respond to such an incident. Traditionally, organizations have focused on prevention, but we now know that early intervention made possible through detection and quick action is necessary to maintain business continuity.

This course will delve into key topics relating to risk/incident definition and categorization analysis, organization and reporting structure, incident response planning and policy development, scenario testing and training. It will cover baseline terminology and concepts related to forming an enterprise incident response team, incident detection, assessment, containment, recovery and communication. Participants will walk away with a useful field guide containing checklists and templates that will improve the organization's ability to rapidly and properly respond to a security incident.

Prerequisite: A general familiarity and working knowledge of information technology, including two or more years of experience and training in IT Audit, Information Security and/or IT

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Information technology professionals especially those in the areas of security, risk, audit and disaster recovery

What You Will Learn

1. **Incident Response Fundamentals**
   - how to recognize and report incidents
   - identification of whether or not an incident has occurred
   - containment of the incident
   - eradication of the threat from the enterprise
2. **Supporting Tools and Technologies**
   - Log Management systems
   - Security Information Event Management systems
   - Vulnerability Management systems
   - endpoint security systems
3. **Incident Policies, Procedures and Training**
   - legal considerations and public communications
   - training your incident response team and end users
4. **Incident Reporting and Post Mortem**
   - analyzing and improving incident response processes
   - reducing incidents through continuous monitoring

SCHEDULE

November 9-10, 2016
New York, NY

March 16-17, 2017
Las Vegas, NV

August 10-11, 2017
Washington, DC

October 26-27, 2017
New York, NY

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ISG320

Managing Mobile Device Security

A Comprehensive Guide to Mobile Security Concepts and Practices

Seminar Focus and Features

Mobility poses many security-related challenges, including anonymous connections, "always on" connections, clear text network traffic, wireless networks and many more. Unfortunately, mobile technology usage in the workplace has grown at a rate that far exceeds the training and education necessary to equip information security professionals to adequately protect their organizations and their end users from mobile-related threats. These professionals are further challenged by the fact that mobile devices are finding their way into the workplace, whether or not the business is ready for them.

This three-day seminar is designed to provide the knowledge and experience you need to enable your organization to securely embrace, deploy and manage mobile devices and applications. Through hands-on exercises you will gain specialized knowledge of mobile technology security. We will cover mobile computing fundamentals, security settings for varying device types, assessing mobile computing risks, developing mobile policies, procedures and standards, auditing mobile devices, deploying and managing a Mobile Device Management (MDM) solution, attacking and defending mobile devices and applications and mobile device forensics.

Prerequisite: Information Security Boot Camp (ISG291), Network Security Essentials (ASG203) or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Information Security and IT Managers; Information Security Analysts, Security Architects, Security Administrators; System Administrators, Network Administrators, IT Auditors; Consultants; Compliance Managers; and anyone who needs a "crash course" in mobile security concepts and practices

What You Will Learn

1. **The State of Security in the Mobile Ecosystem**
2. **Mobile Technology Security Policies**
3. **Network Vulnerability Risk Management**
4. **Mobile Device Management Landscape**
5. **Mobile Platform Vulnerability Risk Management**
6. **Mobile Application Risk Management**
7. **Mobile Data Risk Management**
8. **Mobile Technology Forensics**

SCHEDULE

April 24-26, 2017
Orlando, FL

September 11-13, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2595 **24 CPEs**

Web: misti.com/ISG301

ISG391 NEW!

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. 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 as technologies evolve.

Participants will learn the components of a comprehensive strategy, 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. If you audit 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: None
Advance Preparation: None
Learning Level: Intermediate
Field: Specialized Knowledge & Applications
Delivery Method: Group-Live

Who Should Attend

Information Security Managers, newly appointed CISO's, 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
2. Security Management/ Strategic Components
3. Legislation and Standards
4. Creating a Strong Foundation Through Policy
5. Information Risk Analysis
6. Business Impact Analysis (BIA)
7. Detecting Computer Crime, Accidents, and Errors
8. Physical, Hardware and Environmental Security
9. Awareness Tools
10. Business Continuity Planning (BCP)
11. The Basics of Cryptography
12. The Future of Information Security in the Organization

SCHEDULE

February 27-March 2, 2017
San Francisco, CA

May 1-4, 2017
New York, NY

August 21-24, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/ISG391

ISM230 NEW!

Building an Effective Information Security Program Using Security Frameworks

Strengthen Your Security Program from the Ground Up

Seminar Focus and Features

The increase of global cyber threats have pushed businesses all over the globe to mature their security programs beyond the use of technology alone. To fully understand cyber threats and manage cyber risks, many businesses are waking up to the use of industry defined security frameworks to ensure that an effective information security program is in place.

Because security programs are not "one size fits all," it is crucial that a security framework be used as a starting point and then customized with the business in mind. In this seminar, we will explore how to build an information security program that is appropriate for your organization, in order to protect what is important, manage any foreseeable risks, and meet regulatory compliance.

Prerequisite: None
Advance Preparation: None
Learning Level: Intermediate
Field: Specialized Knowledge & Applications
Delivery Method: Group-Live

Who Should Attend

Information Security Managers, Security Risk Managers, IT Managers, Chief Information Officers, Chief Information Security Officers, anyone who is responsible for information or cyber security within their organization

What You Will Learn

1. What Exactly is a Security Program
2. Using Security Frameworks
3. Identifying What to Protect/ Categorizing Information
4. Using a Governance Structure
5. Defining the Rules with Policies, Standards and Procedures/Guidelines
6. Vendor Security Management
7. Managing Risk with Continuous Monitoring
8. Staying Current
9. Importance of Communicating
10. System Support

SCHEDULE

March 9-10, 2017
San Francisco, CA

June 8-9, 2017
Boston, MA

October 19-20, 2017
Chicago, IL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ISM230

Business Continuity Planning and Disaster Recovery Assurance Practices

Maintaining Service Level Capabilities During Disruptive Events

Seminar Focus and Features

In this two-day course you will learn the objectives of BCP and DR and how they are dependent on one another other for organizational recovery in maintaining service level capabilities during disruptive events. Focus areas in this course consist of the relationship between recovery planning with organizational and functional strategic goals; enterprise governance for BCP including setting BCP priorities and planning; industry compliance requirements; BCP policies, procedures, accountabilities and responsibilities; BCP sequence of plan development and its required components including threat identification, business impact analyses, risk assessment, recovery strategies, resource preparation, testing, returning to normal or the "new normal." Supporting topics will also be addressed, such as the human factors that enable recovery, third-party relationships and organizational synchronization of BCP and incident response planning.

***NOTE:** Attendees will receive a Checklist for ISO 22301 compliance standard.*

Prerequisite: None

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Application

Delivery Method: Group-Live

Who Should Attend

Information Security Managers and Directors; IT Auditors; Risk Managers; CIOs; Consultants; Compliance Managers

What You Will Learn

1. **BCP vs. DR Objectives**
   - acceptable service level requirements when operating under disruption
   - required organizational need and it and departmental support for achieving BCP success
2. **Understanding IT Service Levels to Achieve**
3. **Determining What's Realistic and Reasonable for Your BCP**
4. **BCP/DR Relationship To Business And Strategic Alignment**
   - BCP development to achieve strategic objectives
5. **BCP/DR Responsibilities and Accountabilities**
   - organizational priorities for planning
   - policy and procedural guidance
   - current resources
   - organizational ownership
   - departmental ownership
   - individual responsibilities and accountabilities
   - synchronizing the BCP planning to deliver an effective plan
6. **Industry Specific Guidance**
   - financial services–FFIEC and GLBA
   - healthcare–HIPAA
   - PCI
   - government
   - joint guidance–SEC, FINRA, CFTC
7. **Sequence of Plan Development Process**
   - define ownership for overall plan components and development, maintenance, testing, implementation, return to normal processes
   - threat ID and analysis
8. **Risk Assessment and BIA**
   - translating the threats above into business risks
   - ranking for appropriate treatment
   - potential BCP planning via risk assessment methodology
9. **Recovery Strategies**
   - planning business unit recovery strategies to recover from risk events identified
   - associated business impacts strategically driven within departmental plans
10. **Planning Contingencies to Support Recovery Strategies**
    - determine realistic contingencies to achieve objectives based on understanding of requirements, capabilities, resources and known dependencies and any gaps
11. **Planning for Resources to Support Recovery Strategies and Contingencies**
    - recognizing all dependencies regarding resources of all types to enable success for BCP implementation
12. **Communicating and Training**
    - BCP information dissemination addressing who, what, when and why
13. **Maintaining Information Security in a Disrupted Environment**
14. **Test Planning and Execution**
    - plan completeness
    - ensuring effectiveness of tests
    - testing with partners
    - integrated testing
    - test reporting
15. **Integration of Incident Response Testing with BCP**
    - recognizing regulatory requirements of incident response
    - benefits of leveraging the testing processes
16. **Presented in a Timeline Requiring Use of the Materials Presented:**
    - performing risk identification and analyses
    - risk assessment methodology
    - risk treatment
    - risk mitigations
    - performing business impact analysis
    - understanding and using RTO (Recovery Time Options) for recovery planning
    - identifying and managing dependencies
    - ensuring dependencies are understood regarding recovery strategy.
    - business unit recovery strategy analyses and planning.
    - resource management and planning - human, technological, supplies, facilities, etc., as needed (back up HW, SW, data, redundant human resources, etc)
    - BCP with outsourced processes and vendor relationships
    - hot sites
    - cold sites
    - integrated testing
    - vendor management for BCP
    - test planning and execution
    - determining acceptability of results
    - reviewing third-party results
    - assurance of acceptability of third-party results based on vendor management program
    - documenting the plan
    - executive and board "to dos"
    - minimum documentation requirements
    - training the staff
    - preparing for regulatory or audit review
    - human aspect of BCP/DR
    - realistic controls
    - lists to have
    - tools and references

SCHEDULE

November 14-15, 2016
Boston, MA

March 23-24, 2017
Orlando, FL

June 22-23, 2017
Washington, DC

November 2-3, 2017
Boston, MA

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ISG240

Audit and Security of SAP® ERP

HANDS-ON

Controlling and Managing Risks in SAP R/3 and SAP ECC Systems

Seminar Focus and Features

In this four-day, hands-on seminar, attendees will investigate the risks inherent in the SAP® application and review some of the most effective control opportunities one can configure or design into the application. We will cover the critical business processes required to ensure that SAP is working as intended and that processes/monitoring procedures support effective system control. 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 this seminar we will pinpoint the risks related to default IDs, profile parameters, IMG configuration and maintenance and segregation of duties. We will drill down to core business processes, including the financial close cycle (supported by FI/CO), the order-to-cash cycle (supported by SD), and the purchase-to-pay cycle (supported by MM). Within these modules, attendees will review critical configuration settings such as field status groups, validation routines, posting and payment tolerances, stochastic blocking, dual control over sensitive fields, minimum pricing conditions and automatic credit checking. We will discuss (and show) key risks and controls within other modules and functions that may be of interest.

In addition, participants will explore where SAP is headed with its SAP Governance, Risk and Compliance (GRC) suite of applications, and review the auditing and monitoring changes required to move down this path. You will learn how to structure your implementation or upgrade to avoid common audit issues post "go-live." We will delve into advanced auditing techniques supported by tools within the standard SAP application, including the Audit Information System (AIS) as well as 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 systems 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 Overview and Concepts**
   - terminology
   - SAP naming conventions
   - ERP Central Component and NetWeaver Architecture
   - general SAP controls and risks
2. **SAP Audit Fundamentals**
   - ERP systems: audit implications
   - high-level approach for auditing SAP
   - using a process-based approach
   - example audit recommendations and tips
3. **Basic Navigation for Auditors**
   - running transactions and reports
   - selecting field values
   - browsing tables
   - reviewing configuration settings
   - Audit Information System (AIS)
4. **SAP Security**
   - security overview and key risks
   - system parameters
   - other password-related settings
   - SAP authorization concept
   - key steps to auditing SAP security
   - security best practices
5. **SAP Administration and Change Control**
   - basis functional overview
   - ABAP/4 Workbench
   - Implementation Management Guide (IMG)
   - Computer Center Management System (CCMS)
   - Transport Management System (TMS)
   - managing change
   - dealing with emergencies
   - key risks
   - primary audit activities
   - tips for achieving strong change management
6. **SAP Modules**
   - FI: Financials
   - CO: Controlling
   - MM: Materials Management
   - SD: Sales and Distribution
   - PP: Production Planning
   - HCM: Human Capital Management
   - BI Business Warehouse
   - other modules
7. **FI: Financials and CO: Controlling Risks and Controls**
   - configured control opportunities
   - other process-related controls
   - useful reports and security considerations
8. **MM: Materials Management Risks and Controls**
   - configured control opportunities
   - other process-related controls
   - useful reports and security considerations
9. **SD: Sales and Distribution Risks and Controls**
   - configured control opportunities
   - other process-related controls
   - useful reports and security considerations
10. **Other Modules (based on class interest)**
11. **SAP Governance Risk and Compliance (GRC) Solutions**
    - SAP Risk Management
    - SAP Access Control
    - SAP Process Control
    - SAP Global Trade Services
    - SAP Fraud Management
    - SAP Audit Management
12. **Advanced SAP Auditing Techniques**
    - audit challenges
    - advanced audit tools within and outside SAP
    - transactional analysis opportunities
    - using advanced audit analytics tools: IDEA and ACL
13. **Implementations and Upgrades**

SCHEDULE

October 4-7, 2016
Denver, CO

November 14-17, 2016
Washington, DC

January 23-26, 2017
Phoenix, AZ

March 28-31, 2017
New York, NY

May 8-11, 2017
Orlando, FL

August 14-17, 2017
Chicago, IL

October 2-5, 2017
Washington, DC

December 18-21, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2895 **32 CPEs**

Web: misti.com/ASE241

ASE441

Advanced SAP® ERP Audit and Security

SAP ECC Basis System Settings and Secure SAP Netweaver Configuration®

Seminar Focus and Features

By attending this course, attendees will acquire the knowledge and skills to progress beyond the basic auditing employed by many auditors for SOX purposes, and become competent at an advanced auditing level to identify more in-depth operational and strategic risks. 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. Participants will explore newer issues around SAP cybersecurity, and see demonstrations of techniques used for hacking SAP. Participants will advance their knowledge through hands-on access to an SAP system, and get a chance to perform a mini security audit.

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 Auditors; Audit Managers (responsible for audit planning); SAP Security Administrators; SAP Basis Methodology

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. Special Considerations
6. SAP Authentication Issues
7. Netweaver Security
8. Advanced Auditing of SAP Customizations
9. Hacking SAP (aka: Hardening SAP Against Hacking)
10. Analyzing SAP Tables

SCHEDULE

September 14-16, 2016
New York, NY

April 19-21, 2017
San Francisco, CA

September 19-21, 2017
New York, NY

Available In-House (page 8).

Tuition $2595 **24 CPEs**

Web: misti.com/ASE441

ASE351

HANDS-ON

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. Database Record Mechanisms
6. Integrity Features
7. High-Risk Commands and Utilities
8. Organizational Impact
9. Audit and Security Approaches
10. Wrap-Up

SCHEDULE

September 12-15, 2016
Chicago, IL

May 8-11, 2017
Chicago, IL

November 27-30, 2017
Orlando, FL

Available In-House (page 8).

Tuition $2495 **32 CPEs**

Web: misti.com/ASE351

ASE355

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 a several 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 and 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
7. Application Security Best Practices
8. Change Management Best Practices for Oracle E-Business Suite
9. Designing and Auditing Application Controls
10. Best Practices for Protecting Sensitive Data
11. General Ledger: Risks and Controls
12. Assets: Risks and Controls
13. Cash Management: Risks and Controls
14. Procure to Pay: Risks and Controls
15. Order to Cash: Risks and Controls
16. Inventory: Risks and Controls

SCHEDULE

December 12-14, 2016
San Francisco, CA

April 24-26, 2017
New York, NY

October 9-11, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ASE355

ASG231

HANDS-ON

Securing and Auditing Your Network Infrastructure: Network Services, Devices, and Perimeter Security

Assessing Your Network Security - Inside and Out

Seminar Focus and Features

Over the years, the topic of auditing networks has often been misunderstood and viewed as a technical mystery. In this down-to-earth, no nonsense, 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, attendees will be guided 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 you go back to the office to apply those lessons.

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

Prerequisite: Intermediate IT Audit School (ITG241), Network Security Essentials (ASG203) or equivalent knowledge 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. Securing and Auditing Network Devices
3. Securing and Auditing Wireless Networks
4. Securing and Auditing DMZ Networks
5. Access Control Lists
6. DMZ Audit Planning

SCHEDULE

October 31-November 4
New York, NY

March 20-24, 2017
San Francisco, CA

June 26-30, 2017
Washington, DC

September 25-29, 2017
Anaheim, CA

October 30-November 3, 2017
New York, NY

Available In-House (page 8).

Tuition $3095 **40 CPEs**

Web: misti.com/ASG231

ASG232

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

HANDS-ON

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 for IT Audit and Security Professionals**
2. **Securing and Auditing Operating Systems and Other System Software**
3. **Securing and Auditing Web Application Security**
4. **Securing and Auditing Database Management Systems**

SCHEDULE

February 6-10, 2017
San Francisco, CA

May 1-5, 2017
Boston, MA

July 21-25, 2017
Anaheim, CA

December 18-22, 2017
Atlanta, GA

Available In-House (page 8).

Tuition $3095 **40 CPEs**

Web: misti.com/ASG232

ASN304

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. Attendees will leave this week long seminar with an advanced understanding of how to secure and audit virtualized environments within their own organizations.

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. **ESX Basics**
3. **Hyper-V and Disaster Recovery**
4. **Developing an Audit Program for ESX**
5. **ESX Case Study**

SCHEDULE

October 24-28, 2016
New York, NY

May 1-5, 2017
Boston, MA

August 14-18, 2017
Chicago, IL

November 27-December 1, 2017
San Francisco, CA

Available In-House (page 8).

Tuition $2895 **40 CPEs**

Web: misti.com/ASN304

Audit and Security for Cloud-Based Services

Security and Control Considerations for Cloud Computing Architectures

Seminar Focus and Features

Offering internet-based computing and on-demand resources, software, and data, cloud-based services are rapidly changing the landscape of IT. With Software-as-a-Service (SaaS) delivering application software, Platform-as-a-Service (PaaS) available to design and develop software, and Infrastructure-as-a-Service (IaaS) providing the equipment upon which to support other services, cloud computing offers IT a way to increase capacity and capabilities minus a huge investment.

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. The 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

TOP 10 IN-HOUSE

Who Should Attend

Operational, Business Application, Information Technology and External Auditors; Audit Managers and Directors; Information Security professionals

What You Will Learn

1. **Cloud-Based Computing: An Architectural Overview**
   - application architectures
   - the SPI Cloud Computing Model
   - key drivers for moving towards cloud-based services
2. **Software-as-a-Service (SaaS)**
   - key enterprise applications
   - the SaaS transaction model(s)
   - SaaS security and audit concerns
3. **Platform-as-a-Service (PaaS)**
   - major development providers/ platforms
   - PaaS security and audit concerns
4. **Infrastructure-as-a-Service (IaaS)**
   - host security in the cloud
   - network security in the cloud
   - data storage/SAN in a cloud IaaS environment
   - cloud bursting
   - virtualization models for cloud-based services: Hypervisor VM and inter VM isolation
   - cloud-based security domains: virtualized security/firewalls
   - IaaS security and audit concerns
5. **Cloud-Based Network Models**
   - private cloud architectures
   - hybrid architectures
   - public architectures
   - de-perimiterization of networks: secure access from any device, anywhere
6. **Brokered Cloud Services**
   - cloud aggregators
   - cloud brokers
   - cloud management service portals
7. **Security-as-a-Service**
   - identity management as a service
   - security event monitoring/IDS as a service
   - vulnerability management as a service
   - data leakage prevention as a service/web filtering, e-mail filtering
8. **Cloud-Based Security Standards and Dependencies**
   - directories and identity management
   - federated identities
   - security standards: SPML, XACML, OAuth, OpenID, others
9. **Governance in a Cloud Services Environment**
   - key performance indicators
   - audit trails for cloud-based services
   - service level agreements, licensing
   - legal complexities: data privacy, globalization, trans-border constraints
   - third-party assessments and certifications: SAS70, ISO 27001
10. **Disaster Recovery in a Cloud-Based Environment**
    - SPI HA architectures
    - virtualized environments and the impact on disaster recovery
    - updating and testing disaster recovery plans
11. **Cloud Security and Audit**
    - key risks and audit concerns
    - identifying key controls and mitigations
    - cloud-based risk analysis models: ENISA, NIST, CSA
    - security best practices models for cloud-based services
    - audit techniques and tests in a cloud-based environment

SCHEDULE

September 26-27, 2016
New York, NY

December 8-9, 2016
Chicago, IL

April 27-28, 2017
Boston, MA

June 8-9, 2017
San Diego, CA

August 10-11, 2017
Washington, DC

October 16-17, 2017
Chicago, IL

Available In-House (page 8).

Tuition $1795 **16 CPEs**

Web: misti.com/ASN305

"Great depth of knowledge and ability to teach and relate to our roles. Took time to address all questions."

Navid Ahrarian,
Internal Auditor – Technology,
Fannie Mae

Auditing Encryption

Strengthening the Use of Encryption in Your Organization through Best Practices

Seminar Focus and Features

Encryption: Companies use it, but does anyone outside the security team truly understand it? How do organizations know it's working? Is there a way to know for certain it's protecting the assets it should?

Hackers exploit encryption weaknesses to infiltrate systems and steal sensitive data from businesses–and the companies make the headlines. While encryption is a powerful tool to help protect organizations and the valuable information contained within them, it, like any other technology, isn't foolproof and shouldn't be blindly trusted. As the auditor, it is your job to make sure encryption is properly implemented, maintained and living up to its promise. But how do we audit encryption?

In this three-day course, we demystify encryption to the benefit of auditors, trusted sources, IT managers and users. We explain best practices, risks and how to audit. This course examines the technology to identify both the strengths and weaknesses of commonly used encryption.

You will learn how to identify, evaluate and test encryption within your IT environment for data transmissions and for data at rest, which come with different risks and different encryption requirements. Attend this course and learn how you can review, evaluate and protect your organization before you get attacked.

Prerequisite: None

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Delivery Method: Group-Live

Who Should Attend

Operational, Business Application, Information Technology and External Auditors; Audit Managers and Directors; Information Security professionals

What You Will Learn

1. **Recent Encryption Hacks**
   - hack and encryption key
   - top 10 hacking groups
   - recent hacks and what caused them
2. **Basics on Cryptography Algorithms and Technologies**
   - encryption concepts
   - cracking encryption keys
   - OSI 7-Layer architecture
   - TCP/IP
   - IPv6
   - transmission encryption for business partners
   - Secret (Symmetric Key)
   - Public (Asymmetrical Key)
   - Digital Signature
   - Hash Function
   - Public Key Infrastructure (PKI)
   - Certificate Authorities (CAs)
   - transmission encryption for "casual" users
   - Virtual Private Network (VPN)
   - HTTPS
   - Secure Socket Layer (SSL)
   - Transport Layer Security (TLS)
   - encryption algorithms
   - data-at-rest encryption
   - encryption key management
3. **Identify Access Management**
4. **Encryption: Risks and Best Practices**
   - the technology behind encryption
   - basic concepts and controls
   - OSI 7 layer architecture–key to encryption
   - confidentiality
   - data integrity
   - authentication
   - non-repudiation
   - certificates of trusted partners
5. **Auditing Encryption Key Management**
   - trusted sources
   - separation of duties
   - rotation and cryptoperiods
   - encryption key storage
6. **Auditing Encryption of Data Transmissions**
   - business partners
   - casual users
   - customers
   - public key/private key
   - SSL–the good, the bad, and the ugly
   - distribution of encryption keys
7. **Auditing Encryption of Data-at-Rest**
   - here is where hacking happens
   - data classification systems–benefits and limitations
   - what to encrypt (hint: not everything!)
   - key management and mismanagement
   - monitoring encryption
   - catching the successful hacks
8. **Reducing Cloud Insecurity with Encryption**
   - don't count on the cloud service provider
   - protect your information
   - cloud risks
   - Infrastructure as a Services (IaaS)
   - Platform as a Service (PaaS)
   - Software as a Service (SaaS)
9. **The Future of Encryption**
   - where all this is headed
   - new vulnerabilities
   - will encryption eventual fail?
10. **If You Were Hacked**
    - background information
    - how to catch the successful hack

SCHEDULE

October 12-14, 2016
Boston, MA

March 13-15, 2017
Las Vegas, NV

June 12-14, 2017
New York, NY

September 25-27, 2017
Chicago, IL

Available In-House (page 8).

Tuition $2195 **24 CPEs**

Web: misti.com/ASN311

Securing and Auditing Windows® Active Directory Domains

HANDS-ON

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 and Consultants

What You Will Learn

1. **Windows and Windows Networks**
   - Windows operating systems and versions
   - Windows patches
   - Windows server builds
   - vLANs
   - siloing
2. **Auditing Active Directory Core Components**
   - domains, trees and forests
   - Active Directory structure
   - Active Directory sites and services
   - domain controllers
   - DNS
   - time configuration
   - Active Directory domains and trusts
   - Active Directory federation services
   - Active Directory Certification Authority
3. **Auditing Active Directory Users**
   - user accounts
   - Windows services
   - Active Directory administrative center
   - Active Directory recycle bin
   - authentication policies
   - authentication policy silos
4. **Auditing Active Directory Groups**
   - group types
   - access control lists
   - auditing domain groups
5. **Auditing Password Policies**
   - Security Identifiers (SIDs)
   - kerberos
   - password attack techniques
   - protecting passwords
   - password policies
   - fine grained password policies
6. **Auditing Folder Rights**
   - share permissions
   - NTFS permissions
   - inheritance
   - folder structure and permissions
   - drive mappings
   - best practices
   - identify sensitive folders
7. **Auditing Active Directory Delegation**
   - reasons to delegate the administration of Active Directory
   - Active Directory administration delegation
   - audit Active Directory delegation
8. **Security Compliance Manager and Group Policy**
   - Microsoft Security Assessment Tool 4.0
   - Microsoft Baseline Security Analyzer 2.2
   - Microsoft Security Compliance Manager (SCM)
   - Group Policy
9. **Auditing User Rights and Event Viewer Logs**
   - user rights
   - auditing event viewer logs
10. **Hardening Active Directory**
    - password policies
    - patch management
    - upgrade domain controllers to Windows Server 2012 R2
    - multifactor authentication
    - authentication policy silos
    - silo your network
    - audit administration account use
    - limit membership of schema admins and enterprise admins groups
    - use separate administrative accounts
    - continuous monitoring
    - end user training
11. **Active Directory Case Study**

SCHEDULE

November 1-4, 2016
New York, NY

March 27-30, 2017
Atlanta, GA

May 15-18, 2017
Washington, DC

August 1-4, 2017
Anaheim, CA

October 23-26, 2017
New York, NY

Available In-House (page 8).

Tuition $2895 **32 CPEs**

Web: misti.com/AS0402

"Extremely thorough and expansive details on best practices for securing and auditing active directory. Instructor was extremely knowledgeable and able to easily explain relevant topics."

Chris Myers,
Senior IT Auditor,
American Financial Group

ACL CERTIFIED TRAINING

Capitalizing on Synergies to Bring a More Robust Offering to Our Customers

ACL Analytics is a tool that allows auditors and others to perform data analysis for the purpose of gaining greater insight into the accuracy and validity of corporate data by ensuring it was transacted in compliance with internal policies and procedures and/or 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 & 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&500, Global 500, etc
- Government Agencies – Federal & State

In April 2016 MISTI announced a new partnership with ACL, a technology company focused on the global fraud detection, anti-bribery and corruption and regulatory compliance markets, to deliver high-quality classroom training in North America. ACL users can now attend instructor-led, open-enrollment classroom training delivered regionally for all user levels.

Behind the Partnership

"Customer intensity is one of ACL's three core values, and this partnership with MISTI will allow us to provide local, classroom-based enablement to our customers that would not otherwise be possible. MISTI was the obvious choice–we trust the quality of training they offer and, together, we can provide a richer educational opportunity for our customers to help them become the most sought-after leaders within their organizations."

Sean Zuberbier, Vice President,
Global Sales and Customer Success, ACL

"We are extremely pleased to partner with ACL to provide customers with our unique classroom experience and world-class instructors. Together we can help businesses leverage technology to solve problems and improve their governance, risk and compliance functions. Our industry-leading training is a perfect fit with ACL's technology to provide business leaders with the tools and strategies they need to succeed."

Tony Keefe, President & CEO, MISTI

About ACL

ACL is a Vancouver-headquartered technology company focused on the global fraud detection, anti-bribery and corruption, and regulatory compliance markets. Named as one of Canada's Top SME Employers and a BC Top Employer, ACL helps the world's largest public and private companies stamp out fraud, operational waste and unethical business. With more than 14,000 customers globally, including 89% of the Fortune 500, ACL is changing the entire landscape of the industry by leading auditors, risk and compliance professionals into the cloud and mobile. Visit us online at www.acl.com.

To learn more about ACL training and customer enablement, please visit:
www.acl.com/products/training-and-enablement

 NEW!

ACL™ 101 Foundations

HANDS-ON

Efficiently and Effectively using ACL Analytics to Achieve Your Analysis Objectives

Seminar Focus and Features

This three-day ACL Certified course is a comprehensive introduction to ACL Analytics, designed for new and beginner users who want to learn the concepts and features needed to start using ACL Analytics. In an interactive hands-on environment, you will learn fundamentals such as basic data concepts and how to work within the ACL Analytics environment, as well as integral skills such as how to conduct analysis steps and procedures and accomplish analysis objectives in ACL Analytics. You will learn the proper methodology and best practices for all five phases of the data analysis cycle (planning, importing, preparing, analyzing, and reporting). On the third day, basic scripting will be introduced. Through this comprehensive introduction and practical application, you will learn how to effectively use ACL Analytics to accomplish your audit and/or business objectives.

Learning Objectives

- Reduce time and resources needed to analyze data
- Detect gaps and control failures
- Leverage hundreds of built-in data analysis commands and tools
- Access and reconcile data from various systems in order to identify potential issues
- Identify outliers and issues
- Analyze data to achieve objectives
- Combine data from multiple source types in order to make comparisons between them
- Identify trends between issues that may be indicative of the root cause(s) of the problem
- Create working paper documentation detailing your objectives, the analysis steps taken to achieve them, and the results returned
- Use basic scripting to automate processes and initiate continuous monitoring

Prerequisite: Minimal or no experience with ACL Analytics

Advance Preparation: None

Learning Level: Basic

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Internal and External Auditors; Fraud Examiners; Finance and Accounting Professionals; Information Technology Professionals

What You Will Learn

1. **Basics**
   - data concepts
   - ACL Analytics
     - The Launcher
     - The ACL Analytics environment process
     - ACL Analytics user interface
     - The ACL Analytics environment
     - views/folders/commands
     - datetime and numeric display formats
   - phases of data analysis
2. **Expressions**
   - filters
     - global view filters
     - creating filters using the expression builder
     - unconditional/conditional computed fields
     - functions
     - expression features
     - fixed-point arithmetic
3. **Importing Data**
   - locate/acquire files
   - source file formats
   - import files
   - verifying validity
   - SQL syntax
   - reusing layouts
   - refresh from source
   - reusing log import entry
4. **Preparing Data**
   - integrity threats
   - controls
     - preparation checklist
   - bounds testing
   - quality and completeness
   - uniqueness
     - measuring reasonableness
     - association and recalculation
5. **Analyzing Data**
   - grouping data
     - CLASSIFY/SUMMERIZE commands
     - CROSS-TAB command
     - STRATIFY command
     - AGE command
   - reordering records
     - quick sort
     - SORT command
     - INDEX command
   - isolating data
   - combining data
     - using EXTRACT/APPEND
     - using EXPORT/APPEND
     - JOIN command/processes
     - planning checklist
     - join types
6. **Reporting**
   - EXPORT Command
   - The Log
     - log sessions and entries
   - visualizing data
     - The Analysis App window
     - interpretations
     - filtering and sorting data
     - breaking down the bubble chart
   - results manager
     - sharing and tracking
     - assign access
     - automate the process
     - create a storyboard
7. **Scripting**
   - command syntax
   - creating a script
   - SET command
   - OPEN command
8. **Variables**
   - variable creation
   - variable permanency
   - interactive scripts
9. **Variable Substitution**
   - adding comments to scripts
   - computed fields and functions
   - unconditional computed fields
   - conditional computed fields
   - functions
10. **Appendices**
    - hex to ASCII conversion table
    - hex to EBCDIC conversion table
    - many-to-many join process
    - about results manager
    - additional resources

SCHEDULE

September 12-14, 2016	Costa Mesa, CA
September 26-28, 2016	Dallas, TX
October 11-13, 2016	Boston, MA
October 24-26, 2016	Chicago, IL
November 14-16, 2016	Washington, DC
December 5-7, 2016	San Francisco, CA
January 23-25, 2017	Houston, TX
February 13-15, 2017	New York, NY
March 6-8, 2017	Atlanta, GA
April 3-5, 2017	Chicago, IL
April 24-26, 2017	Dallas, TX
May 8-10, 2017	San Francisco, CA
May 22-24, 2017	Washington, DC
June 19-21, 2017	New York, NY

Tuition $1800 **25 CPEs**

Web: misti.com/ACL101

ACL201 NEW!

ACL™ 201 Applications

HANDS-ON

Identify and Apply the ACL Analytics Functionality Needed to Achieve Desired Objectives

Seminar Focus and Features

This two-day course is a practical application of ACL Analytics, designed for users who want to use ACL Analytics more effectively in real-life situations. By working through a series of progressively challenging case studies, you will develop your critical thinking and application of ACL Analytics. In an interactive, hands-on environment, your ACL Certified trainer will teach you to accomplish data analysis tasks of varying complexity through the integration of ACL commands and expressions. Through this practical application, you will learn how to effectively separate objectives into manageable milestones and enhance your effectiveness with ACL Analytics.

Learning Objectives

- Apply ACL Analytics in a structured data analysis process
- Critically determine and assess objectives and planning analysis
- Separate objectives into intuitive milestones
- Prepare data for analysis
- Test issues to identify trends that may be indicative of cause(s) of them
- Create working paper documentation showing your objectives and results

Prerequisite: ACL 101 Foundations course or self-taught to comparable level

Advance Preparation: None

Learning Level: Intermediate

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Internal and External Auditors; Fraud Examiners; Finance and Accounting Professionals; Information Technology Professionals

What You Will Learn

1. **Review**
2. **Structure**
3. **Case Studies**
   - sales commissions
   - accounts payable
   - procurement cards
   - travel and entertainment
   - PBX phone charges

SCHEDULE

September 15-16, 2016
Costa Mesa, CA

September 29-30, 2016
Dallas, TX

October 27-28, 2016
Chicago, IL

December 8-9, 2016
San Francisco, CA

January 26-27, 2017
Houston, TX

March 9-10, 2017
Atlanta, GA

May 11-12, 2017
San Francisco, CA

June 22-23, 2017
New York, NY

Tuition $1450 **16 CPEs**

Web: misti.com/ACL201

ACL303 NEW!

ACL™ 303 Scripting

HANDS-ON

Create Simple and Interactive Scripts to Implement Automated Routines, Continuous Monitoring and Gain Further Insight into Your Data

Seminar Focus and Features

In this three-day course, you will learn how to use ACL Analytics functions and scripts to gain new insight into your data and do more in less time. Functions let you investigate your data in ways you haven't thought of before, adding power and detail to your analysis. Scripts let you automate routine ACL Analytics tasks, freeing up time to concentrate on activities that require critical thinking and judgment. Scripts also help preserve best practices, which prevents errors, and results in better controls in your organization. ACL Certified trainers will show you how to implement scripts into your daily routine, and they will guide you through activities that illustrate how to work with scripts and functions efficiently and easily.

Learning Objectives

- Apply ACL commands and functions to perform parsing and harmonization of complex fields
- Apply ACL commands and functions to search for matching data

Prerequisite: ACL 201 Applications course or at least six months previous experience using ACL Analytics

Advance Preparation: None

Learning Level: Advanced

Field: Specialized Knowledge & Applications

Delivery Method: Group-Live

Who Should Attend

Internal and External Auditors; Fraud Examiners; Finance and Accounting Professionals; Information Technology Professionals

What You Will Learn

1. **Basics**
2. **Importing**
3. **Analyzing**
4. **Structured Scripts**
5. **Advanced Topics**

SCHEDULE

September 26-28, 2016
Dallas, TX

October 24-26, 2016
Chicago, IL

November 14-16, 2016
Washington, DC

February 13-15, 2017
New York, NY

April 24-26, 2017
Dallas, TX

Tuition $2100 **25 CPEs**

Web: misti.com/ACL303

SEMINAR FACULTY

Candy Alexander, CISSP, CISM, Cyber Security and Information Security Executive - Independent Consultant

Anthony J. Bellezza, CPA, Sr. Vice President & Chief Compliance Officer, Rite Aid

Steve Biskie, CISA, CITP, CPA, CGMA, Co-Founder, High Water Advisors

Ann M. Butera, CRP, Founder & President, The Whole Person Project, Inc.

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

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

Kathleen Crawford, Sr. Consultant, MIS Training Institute

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, MIS Training Institute

Mark T. Edmead, MBA, CISA, CISSP, IT Transformation Consultant, MTE Advisors; Sr. Instructor, MIS Training Institute

Shawna M. Flanders, CRISC, CISM, CISA, CSSGB, SSBB, Founder & CEO, Business Technology Guidance Associates, LLC

Martin H. Green, Esq., Sr. Instructor, MIS Training Institute

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

Ken Jaworski, CISSP, CIPP, CIPM, Data Security Specialist, Lochbridge Professional Services

Kevin Johnson, Chief Executive Officer, Secure Ideas

Stephen Kost, Chief Technology Officer, Integrigy Corporation

Joel F. Kramer, CPA, Managing Dir., Internal Audit Division, MIS Training Institute

Susan M. Landauer, CPA, Firm Partner, Forensic Accounting Services Group, LLC

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

Dr. Hernan Murdock, CIA, CRMA, Vice President, Audit Division, MIS Training Institute

William J. Nealon, CIA, CFE, Sr. Consultant, MIS Training Institute

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

Fred C. Roth, CISA, Vice President, Audit Division, MIS Training Institute

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

Elizabeth Sandwith, CFIIA, Partner, Sandwith Internal Audit Services

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

Marilyn Stanton, MSOD, Managing Partner, Illuminated Consulting LLC

Alan Sugano, President, ADS Consulting Group, Inc. (ADS)

Ann Tasby, CPA, CIA, MBA, Governance, Risk and Compliance Executive

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

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

William Woodington, CPA, CIA, President, Woodington Training Solutions, LLC

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

REGISTRATION FORM

CONTACT MISTI CUSTOMER SERVICE FOR:

- Inquiries regarding discounts, certificate programs, training weeks and multiple registrations
- Convenient registration over the phone or email
- Help identifying the right training for you
- CPE questions

Name* ☐ Mr. ☐ Mrs. ☐ Ms. ☐ Dr. ☐ Prof. Name for Badge

Job Title* E-Mail Address*

Company/Organization* Industry

Address* Mail Stop/Floor

City* State/Province* Zip + 4/Postal Code* Country*

Telephone* Fax

Supervisor Title

1. Seminar Title* Seminar Code

Location* Date*

2. Seminar Title* Seminar Code

Location* Date*

*Fields noted with an *asterisk are required. Please print clearly.*

CISSP CERT. #_____

☐ I am enrolling in a Certificate Program seminar

Use of Your Information: The information you provide on this form will be used by MIS Training Institute, Inc. and its group companies ("we" or "us") in relation to your registration for this event. We may also monitor your use of our website(s), including information you post and actions you take, to improve our services to you and track compliance with our terms of use. Except to the extent you indicate your objection below, we may also use your data (including data obtained from monitoring) (a) to keep you informed of our products and services; (b) occasionally to allow companies outside our group to contact you with details of their products/services. As an international group, we may transfer your data on a global basis for the purposes indicated above, including to countries which may not provide the same level of protection to personal data as within the European Union. By submitting your details, you will be indicating your consent to the use of your data as identified above. Further information on our use of your personal data is set out in our privacy policy, which is available at www.misti.com or can be provided to you separately upon request.
Marketing Choices: If you object to contact as identified above by telephone ☐, fax ☐, email ☐, or post ☐, please tick the relevant box. If you do not want us to share your information with other companies, ☐ please tick the box.

To Register

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

Mail List Changes

- ☐ Make indicated corrections to my mailing label (include label)
- ☐ Add me to your mailing list
- ☐ Remove me from your mailing list

Send Information On

- ☐ Conferences/Symposia
- ☐ In-House Training
- ☐ eLearning Training
- ☐ MISTI Certificate Programs
- ☐ MISTI Seminars in Europe
- ☐ MISTI Seminars in Asia
- ☐ PERC (Preferred Education Rate Contract)

Payment Method

Payment due prior to seminar

☐ Check enclosed (*payable to MIS Training Institute*)

☐ MISTI PERC # .....

To pay by credit card, please register online or call Customer Service at (508) 879-7999, ext. 501 and have your credit card information ready.

MIS Training Institute accepts the following credit cards: VISA, MasterCard, AMEX, Diners Club and Discover.

AMOUNT DUE $ .....

Add $100 if registering within 5 business days of session $ .....

TOTAL DUE** $ .....

***See Discounts on page 67. Discounts cannot be combined.*

Connect With Us

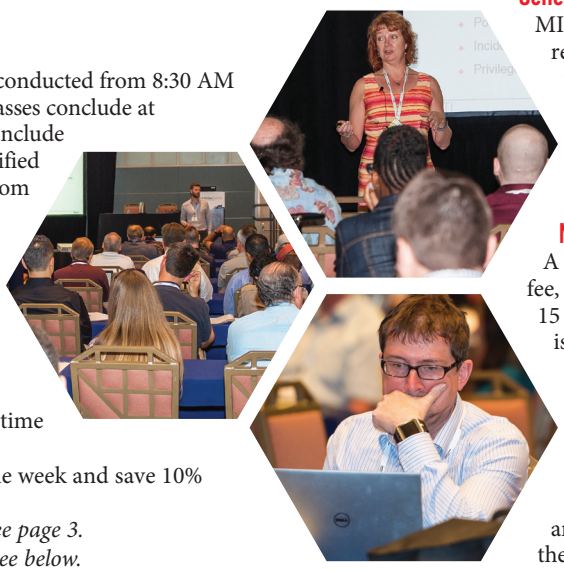
Online www.misti.com
E-mail customerservice@misti.com
Mail MIS Training Institute, 153 Cordaville Road, Suite 200, Southborough, MA 01772-1834
Call (508) 879-7999 ext. 501 **Fax** (508) 787-0033

Tuition

Tuition is listed after each course outline. Add $100 if you register 5 business days or less before the session start date. 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

All MISTI seminars are group-live and 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. All ACL certified courses are group-live and are conducted from 8:30 AM - 4:30 PM daily.



Discounts

(Savings do not apply to already discounted seminars, individual webinars or self-study online training and cannot be combined.)

- Register 3 or more people for the same seminar, same date and save 10%. All registrations must be made at the same time and paid for together.
- Attend consecutive seminars in the same week and save 10% on both seminars.
- Training Week Discounts. *For details, see page 3.*
- PERC: Volume Discounts. *For details, see below.*
- Government: Take 10% off regular fees.

Call Customer Service for more details on discounts.

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.
*Government agencies may submit a P.O. as advance payment.

PERC Dollars	Discount Rate	You Pay	You Save
$15,000	10%	$13,500	$1,500
$20,000	15%	$17,000	$3,000
$30,000	20%	$24,000	$6,000

MISTI Certificate Curriculum

MISTI has developed certificate programs to help Auditors, Information Security professionals and IT Auditors gain the vital skills, confidence and credibility they need to succeed in specialized roles in their respective disciplines. *For details, see page 9.*

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

MISTI may occasionally find it necessary to reschedule, relocate or cancel seminars and will give registrants advance notice of such changes. MISTI will not be responsible for penalties incurred as a result of non-refundable airfare purchases or hotel reservations.

MISTI Cancellation Policy

A full refund, less a $195 administrative fee, will be given for cancellations received 15 days or more before the event. Tuition is non-refundable for cancellations made 14 days or less before the event. You may, however, transfer your tuition to another MISTI event, less a $195 administrative fee. Transfers are valid for 12 months from the time of initial cancellation. Substitutions are welcome at any time. Those who do not cancel before the event date and who do not attend are responsible for the full non-refundable, non-transferable tuition. To cancel, call Customer Service at (508) 879-7999 ext. 501.

CPE Credits

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

MIS Training Institute 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.learningmarket.org

CISSP

Provide your CISSP number on the registration form and we will automatically forward your CPEs to (ISC)² for credit.

High-Yield/No-Risk Guarantee

Attend an 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.

For information about programs in Europe, Middle East, Africa and Asia Pacific:

Phone +44 (0)20 3819 0800 **E-mail** misti@misti.com

MIS|TI™
TRAINING INSTITUTE

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

Registration Code: A816

PRSRT STD
U.S. POSTAGE
PAID
BOLINGBROOK, IL
PERMIT NO. 2216

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 or fax us your mailing label.*

2017
COURSE CATALOG

SEPTEMBER 2016 - DECEMBER 2017

MIS|TI™
TRAINING INSTITUTE
WWW.MISTI.COM

Providing Training Through Knowledge, Insight & Experience

Internal Auditing • IT Auditing • Information Security • Risk-Based Auditing • Fraud Auditing

MIS Training Institute, 153 Cordaville Road, Suite 200, Southborough, MA 01772-1834
Call 508 • 879 • 7999 ext. 501 E-mail customerservice@misti.com