

Training Courses Fiscal Year 2016:
Updated December 2015

5– Operational Auditing

Instructor: Larry Hubbard – Larry Hubbard and Associates

<http://www.lhubbard.com/about.htm>

Date: January 26, 2016

Location: Patrick Henry Building
1st Floor East Reading Room

Address: 1111 E. Broad Street,
Richmond, Virginia 23219

Pricing Terms: \$175.00

CPE: 8 hours

General Overview:

Internal auditors must evaluate controls well beyond the financial reporting and compliance worlds. Some say these operational areas are the most important areas of the organization – I agree! Whether or not you have operational experience, by understanding the roles of management controls and internal control frameworks, you can evaluate and improve the risk management and control processes in the operational areas of your organization. Operational auditing is not consulting, but the skills in this course can help auditors improve processes and position organizations better achieve their objectives.

Course Outline:

Operational Auditing Overview

- Definition of operational auditing
- Operational auditing vs. consulting activities
- The IIA Standards
- Corporate governance, ERM, and internal controls

Management Controls

- The importance of clear objectives
- Tools for achieving objectives - RACI charts, teamwork, SWOT analysis, ISO, TQM, Six Sigma, Balanced Scorecards

Internal Control and Other OA Approaches

- The COSO frameworks
- Applying COSO
- Twelve Attributes of Effectiveness
- Control Self-Assessments

The Audit Model

- The basic audit model: Planning, Performing, Communicating, Monitoring, Quality Assurance
- Risk-based audit planning
- Responsibilities for preventing and detecting fraud
- Interviewing skills
- Five attributes of an audit finding
- Audit reporting and Internal control maturity models

Administration:

No advance preparation or prerequisites are necessary for this course. The program level is basic. The

delivery method is Group-Live and 8 CPE hours in the Auditing field of study are available.

Course Link:

http://www.lhubbard.com/Outlines/Operational_Auditing_Course.pdf

6- Evaluating Your Organization's Fraud Risk Management Program

Instructor: Larry Hubbard – Larry Hubbard & Associates

<http://www.lhubbard.com/about.htm>

Date: January 27, 2016

Location: Patrick Henry Building
1st Floor East Reading Room

Address: 1111 E. Broad Street,
Richmond, Virginia 23219

Pricing Terms: \$175.00

CPE: 8 hours

General Overview:

This course provides a comprehensive approach to evaluating your organization's fraud risk management program. The IIA Standards require internal auditors to evaluate the role of risk management, including that related to fraud risks, in their organization. This course is designed to help you perform that evaluation. In addition to covering the concepts of fraud, the course integrates the roles of risk management, risk-based auditing, continuous auditing and monitoring.

The course is intended for auditors of all levels to provide an in-depth understanding of the terminology, approaches and requirements related to preventing and detecting fraud. The course would also be useful for risk management professionals, and any manager wanting to take a more active role in fraud prevention and detection in their organization.

The course utilizes widely-available reference materials from The Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners.

Course Objectives:

- Provide an understanding of the IIA Standards related to fraud and risk management
- Clarify the terms related to risk management, risk assessment and risk-based auditing
- Learn the barriers to detecting fraud in routine audits
- Discuss role of continuous monitoring and continuous auditing in detection of fraud
- Practice the tools needed to perform an effective fraud risk assessment
- Begin an evaluation of your organization's Fraud Risk Management Program

Course Outline:

The Basic concepts of Fraud Risk Management

- The IIA Standards Related to Fraud
- Risk Management Concepts
- Relation to Risk-Based Internal Auditing
- Risk Terminology: Inherent, Residual, Control, Appetite
- Exercise: The Risk Umbrella

- Types of Fraud Defined by ACFE
- Why Employees Commit Fraud
- Risk Tools: The Risk Register, Risk Matrix and Risk Mapping

The Fraud Risk Management Program

- Fraud Policy for the Organization
- Roles in Prevention, Detection and Investigation (PDI) of Fraud
- Links to Ethics and Values
- Reporting Results of the Fraud Risk Management Program
- Exercise: Documenting the Fraud Program

Performing a Fraud Risk Assessment

- Entity-Level and Activity-Level Approaches
- Identifying Activities and Objectives
- Types of Controls
- The Indicators/Red Flags of Fraud
- The Role of Facilitated Self-Assessment Workshops
- Exercise: Typical Frauds and Their Symptoms

Evaluating Your Organization's Program – Practice Session

- Documenting the Program
- Evaluating Management's Efforts
- Performing a Fraud Risk Assessment
- Building Fraud Detection into Audits
- Reporting Fraud Risk Management Results

Administration:

No advance preparation or prerequisites are necessary for this course. The program level is basic. The delivery method is Group-Live and 8 CPE hours in the Auditing field of study are available.

Course Link:

<http://www.lhubbard.com/Outlines/Evaluating-Your-Organizations-Fraud-Risk-Management-Program-Outline>

7– VITA Audit Security Compliance

Instructor: Edward Miller, Virginia Information Technologies Agency

<https://my.share.virginia.gov/Person.aspx?accountname=COV%5Ctio91281>

Date: February 23, 2016

Time: 9:00 – 3:00

Location: Virginia Information Technologies Agency
The Commonwealth Enterprise Solutions Center (CESC)

Address: 11751 Meadowville Ln
Chester, VA 23836

Pricing Terms: \$0.00 for executive branch and university IT auditors, internal audit directors and IT security officers

CPE: 5 hours

This course is designed for security auditor, agency internal audit director or IT security professional within a state agency responsible for compliance with VITA IT Security Audit requirements.

General Overview:

It is imperative that the Commonwealth of Virginia protect citizen data and provide a safe, secure technology environment that enables state agencies to accomplish their respective missions. VITA's Commonwealth Security & Risk Management Directorate is tasked with fulfilling this mission and in doing so, offers significant benefits to agencies of the Commonwealth. The results citizens are afforded are as follows:

- Confidence in the integrity of the data and the systems processes
- Assistance in compliance with laws and regulation involving confidentiality
- A secure environment in which to perform business activities of the Commonwealth
- Identification and protection of key business functions and services in the event of disaster
- Monitoring for intrusions and Network "attacks" on Commonwealth systems

In order to accomplish its mission, the VITA Commonwealth Security & Risk Management Directorate develops and manages an ever changing portfolio of tools and processes designed to secure Commonwealth data and systems.

This course, provided by VITA will provide Internal Audit and IT Security Departments with insight on VITA IT Security Audit requirements.

Note:

This class will be provided by VITA to help provide guidance related to the VITA IT Security Audit requirements.

Reminder:

This course is being developed with VITA Compliance and the above overview is expected to change to the benefit of the intended audience.

Course Link:

N/A

8 - Incident/Breach Response Management Program Training

Instructor: David Cole – SysAudits.com

<https://www.linkedin.com/pub/david-cole/4a/727/b1a>

Date: March 22, 2016 and March 23, 2016

Location: Virginia Information Technologies Agency
The Commonwealth Enterprise Solutions Center (CESC)

Address: 11751 Meadowville Ln
Chester, VA 23836

Pricing Terms: \$350.00

CPE: 16 hours

General Overview:

This course is intended to provide a general overview of assessing an organization's incident handling and event management program (IHP) as well as information on how to audit the secure configuration of

operating systems and network devices. Attendees will gain an understanding of the NIST Incident Handling framework as well as other best practices for assessing an IHP. Also, attendees will gain insight on technical standards and best practices for securing operating systems and network devices. As part of the subjects covered, the instructor will where appropriate provide audit programs, control framework maps, checklists and case studies. Open LDAP will be addressed as part of this course.

Course Outline:

Incident/Breach Response Management Program

- Overview of current breaches
- Overview of detection and monitoring methods
- Role of SIEM (Security Information and Event Management) systems
- Designing and leveraging external and internal network vulnerability testing with assessment of incident response and breach management program

Auditing and Assessing critical servers and CISCO devices

Overview of enterprise environments: Business data, medical (HIPPA), PCI

- Microsoft
 - MS 2012
 - Microsoft's MS-SQL database 2008 server and
 - MS-IIS
- Oracle/Sun
 - Solaris
 - Oracle
 - Apache
- Assessing Cisco Devices
 - Routers, Switches, and Firewalls

Administration:

No advance preparation or prerequisites are necessary for this course. The program level is basic and is intended for IT Auditors and IT security professionals. The delivery method is Group-Live and 16 CPE hours in the Auditing field of study are available.

Course Link:

N/A

9– Senior Auditor Training Course

Instructor: Various Individuals from State Audit Departments

Date: March 8, 2016

Location: Virginia Commonwealth University
University Student Commons
Salon I-II

Address: 907 Floyd Ave.
Richmond, VA 23220

Pricing Terms: \$0.00 for executive branch agency and university auditors

CPE: 8 hours

This course is reserved for auditors from executive branch and university audit departments. Only 2 auditors per agency will initially be allowed to register for the course. Remaining seats will be made available once each agency has had an opportunity to register for the course.

General Overview:

OSIG is sponsoring a free one day training session for executive branch agency and university senior auditors. The topics covered will be based on input provided from the internal audit directors in the state of Virginia. The intent of this course is to provide senior auditors with best practice training tools in key subject areas that benefit all audit departments. Parking will be provided for all attendees.

Course Topics that will be covered:

- Risk Assessment – the Audit Universe
- Planning an Audit
- Audit Workpapers
- The Benefits of Automation software for Audit Workpapers
- Quality Assurance and Improvement Programs for audit departments
- Report Writing

Note:

This class will have speakers from various state executive branch agency and university audit departments providing useful tools and tips for guiding senior auditors based on their skills and experience.

Parking:

Attendees will be permitted to park in the West Broad Street parking deck (off of Harrison) and will need to pull a ticket to enter the garage. They will be given a parking voucher with a QR code at the event and will scan that when they go to exit the garage once the session has concluded.

Reminder:

This course is being developed with the senior auditors of state agency and higher education needs in mind.

Course Link:

N/A

10– Introduction to Digital Forensics for State Government

Instructors: David Raymond and Randy Marchany
Virginia Tech IT Security Office

<http://www.security.vt.edu/>

Date: April 12, 2016

Location: Virginia Information Technologies Agency
The Commonwealth Enterprise Solutions Center (CESC)

Address: 11751 Meadowville Ln
Chester, VA 23836

Pricing Terms: \$40.00

CPE: 8 hours

Students must have a Wi-Fi enabled laptop with a Windows 7 operating system and VMWare installed to be able to participate in class. Instructors will not be able to load software on the day of class.

Course Overview:

An understanding of digital forensics is essential to the protection of your agency/university in the event of a security breach that involves the loss of confidential information.

This course is designed to deliver a comprehensive introduction to digital forensics and help you develop an effective forensic readiness plan for your organization.

Students will be provided with an instructive overview of the types of information which can be found on computers, mobile phones and other forms of digital media. This includes passwords, Google searches, web surfing history, deleted documents and emails.

Reminder:

This course is being developed with the state agency and higher education needs in mind, and the above overview is expected to change to the benefit of the intended audience.

Prerequisites:

Students will need to have a laptop with VMWare Workstation or VMWare Player installed (Note that VMWare Player is available for free download at www.vmware.com/products/player). Apple computer users should have VMWare Fusion installed. The course includes a VMWare image file of a guest Linux system that is larger than 3GB. Therefore, you need a file system with the ability to read and write files that are larger than 2 GB, such as NTFS on a Windows machine. Initial understanding of what digital forensics is in the IT world is preferred. Some experience using a Linux system is also helpful, although we will provide a quick Linux primer/review as part of the class.

Laptop Requirements

1. Install virtual machine hypervisor (VMware player, VMware Workstation, VMware Fusion for Mac) – requires administrative access to the laptop to accomplish the install, contact your IT administrator for installation.
2. Use the virtual machine hypervisor – the end user will require full control of the VM’s storage folder as part of the IT administrator installation.
3. Load the instructor-provided VM image which will be provided to registrants a few weeks prior to the course

Note: As long as students have some form of VMWare product installed by their IT folks and a functioning USB port, they can also copy the VM from a thumb drive during the first hour or so while we are in lecture mode. Participants’ admin rights are not required unless they need that to copy a file from a thumb drive.

Course Link:

N/A

11– State Updates

Instructor: Various Individuals from State Government

Date: May 24, 2016

Location: Patrick Henry Building
East Reading Room - 1035

Address: 1111 East Broad Street,
Richmond, VA 23219

Pricing Terms: \$0.00

CPE: 8 hours

Reserved for Government Employees impacted by changes to State Policy

Note:

This class will have speakers from various state agencies such as OSIG, DOA, DGS, VITA as well as APA talking about important matters or changes that could affect other state agencies.

Reminder:

This course is being developed with the state agency and higher education needs in mind, and the above overview and will follow the annual state update format performed in prior years.

Course Link:

N/A

12– Performing Self Assessments with Independent Validation using the IIA Self-Assessment Manual

Instructor: Reza Mahbod – RMA Associates, LLC

<http://www.rmaassociates.us/training/>

Date: June 8, 2016

Location: James Monroe Building
22nd Floor Conference Room

Address: 101 N. Franklin Street,
Richmond, VA 23219

Pricing Terms: \$175.00 (early payment) if payment is received prior to May 24th / \$195.00 if payment is received May 24th or later.

CPE: 8 hours

General Overview:

This class will benefit audit shop compliance with the IIA standards, specifically the IIA Standard 1312 requirement. IIA Standard 1312 requires that: **“External assessments must be conducted at least once every five years by a qualified, independent reviewer or review team from outside the organization.”**

Without this external review, an audit department cannot say their work is performed in compliance with the Standards.

While, being able to provide the assurance that your audit department is in compliance with the IIA Standards, may not be required, it has the benefit of strengthening the weight and value of agency audit results. In addition, following the IIA’s Standards provide structure that assist audit departments perform their work.

Course Outline:

- I. Introduction
- II. Overview of Institute of Internal Auditors (IIA)
- III. Quality Assessment & Improvement Programs
 - Internal Assessment
 - Independent Validation
- IV. IIA Standard 1312 Compliance

- V. Principles of Self-Assessment with Independent Validation
 - Internal assessment checklist process
 - Documentation requirements
- VI. Self-Assessment Checklist & Tools
- VII. Self-Assessment Process
 - Planning
 - Complete Checklist
 - Gap Analysis
 - Surveys & Interviews
 - Document analysis and observations
 - Reporting
 - Self-Assessment: The 3 P's

Materials:

Course materials are contained in a participant workbook. A copy of the IIA Standards will be included. Participants may want to separately purchase and bring The IIA Quality Assessment Manual, as that Manual is not supplied as part of the course. The IIA QA Manual is **not** required to complete the course.

Administration:

No advance preparation or prerequisites are necessary for this course. The program level is basic. The delivery method is Group-Live and 8 CPE hours in the Auditing field of study are available.

Course Link:

N/A