aci LEARNING [AUDITPRO]

Course Catalog

Last updated: February, 2023

Be bold.
Train smart.

Table of Contents

On-Demand Solutions

Fundamentals of Internal Auditing

Prerequisite: None

Advance Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Internal and IT Auditors looking for a comprehensive understanding of the process of Internal Audit. This foundational course can be used to onboard rotational Internal Auditors and other experienced professionals starting their careers.

CPE: 24

Overview: In this course, participants will learn traditional and operational auditing concepts, gaining proven tools and techniques for performing effective audits. This course provides insights for conducting internal audits effectively from the initial risk assessment through planning, fieldwork, and reporting. It covers key techniques like flowcharting, preparing risk-control matrices, documenting issues, and writing narratives.

Core Topics:

- Key Concepts of Internal Auditing
- Risk Assessment
- Audit Project Planning
- Document Controls
- Audit Programs
- Fieldwork Techniques
- Verbal Communications
- Workpapers
- Audit Findings
- Written Communications
- Audit Sampling
- Reflecting on Internal Audit's Past and Looking Forward

IT Audit School

Prerequisite: None

Advanced Preparation: None

Learning Level: Entry-Level

Field: Auditing

Who Should Attend: Entry-level IT Auditors and Technologists looking for a foundational understanding of IT auditing

CPE: 32

Overview: This course is for Financial, Operational, Business, and new IT Auditors and provides an in-depth review of the risks and controls of auditing IT and business application systems. Participants will learn about the database, network, business application, transaction risks and controls, end-user computing, assessing control ownership, and how to document and test inputs, processes, outputs, master files, and interfaces.

Core Topics:

- How Is IT Used in Companies?
- IT Risks
- Basics of IT
- Networks
- Internet of Things (IoT)
- Databases
- IT General Controls
- Frameworks and Laws
- Governance
- Application
- Audit Planning

Introduction to Information Security

Prerequisite: None

Advanced Preparation: None

Learning Level: Entry-Level

Field: Auditing

Who Should Attend: Internal Auditors, Compliance Experts, and leaders in Internal Audit departments

CPE: 24

Overview: This course is designed to give those new to Information Security auditing a basic understanding of Information Security key concepts, players, and components. Participants will learn how the Information Security function aligns with the organization's business and strategic objectives. Additionally, the course will highlight methods to provide assurance in the Information Security space and the critical importance of communication. This course will provide the foundational knowledge auditors need to perform Information Security governance audits and basic assessments of Information Security operations.

Core Topics:

- The Security Umbrella Overview
- Information Security Management Basics
- Threats and Vulnerabilities
- Information Security Policy
- Information Security Risk Management
- Assurance
- Security Considerations
- Cryptography
- Communication

Psychology of Fraud

Prerequisite: None

Advanced Preparation: None

Learning Level: Entry-Level

Field: Auditing

Who Should Attend: Internal Auditors, Business Managers, and employees

On-demand Learning Type: Skills

CPE: 6 – Enterprise only

Overview: This course covers proven techniques based on understanding the psychology of fraud to help prevent and mitigate fraud within core business systems. After defining fraud and establishing the universal scope of the problem fraud presents to organizations worldwide, it examines the psychology and motivations of fraudsters to help understand and develop strategies for prevention and detection.

By understanding the psychology of fraud, we will be better able to design fraud prevention, detection, deterrence controls, analysis, and investigations.

This course also includes proven fraud prevention and detection techniques based on an understanding of the psychological factors related to fraud. Armed with a thorough understanding of how psychology impacts behaviors, participants will be better prepared with the knowledge needed to create a more effective anti-fraud environment.

Core Topics:

- Overview and Introduction
- Why Do People Commit Fraud?
- Fraud Prevention
- Fraud Detection
- Psychology of the Aftermath
- Key Takeaways

Ethics in Audit

Prerequisite: None

Advanced Preparation: None

Learning Level: Entry-Level

Field: Auditing

Who Should Attend: Internal Audit staff, Audit Managers, and GRC professionals

CPE: 2

Overview: Internal Auditors must act ethically while reviewing and making recommendations to improve the structures and processes that promote appropriate ethics within their organizations. To do this, they must understand the principles and practices that drive ethical decision-making and the roles that various parties play in setting expectations, monitoring results, rewarding compliance, and correcting deviations. All organizations are under pressure to meet business objectives while managing the variety of ethical views of their diverse stakeholders.

This course provides a solid foundation on the values, organizational structures, roles, responsibilities, and best practices driving ethical conduct in a complex and rapidly changing world, how organizations create the capacity to address new scenarios, and how Internal Auditors can meet their mandate to evaluate the design, implementation, and effectiveness of ethics-related objectives, programs, and processes.

Core Topics:

- Auditor Responsibilities
- Ethical Decision-Making
- Guiding Principles
- Ethical Pillars
- Fraud, Training, and Whistleblowing Programs
- Audit Program Preparation
- Performing the Audit

Auditing Capital Projects

Prerequisite: Fundamentals of Internal Auditing (OAG101)

Advanced Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Internal auditors, compliance professionals, and project managers looking for a comprehensive understanding of the risks and controls around projects, and the project life cycle.

On-demand Learning Type: Skills

CPE: 8 – Enterprise only

Overview: When given a project to audit, the task may seem daunting and impossible. Many will not know where to start. Through this course, students will understand the importance of auditing capital projects and will learn tips and tricks to determine the project's risks and risk mitigation techniques. The course will be a general overview and will enable an auditor to develop an audit workflow, prioritize tasks, and understand how all the pieces of the projects fit into one another. Students will be able to have a more intelligent conversation with the project management staff, as some common terms will be defined in the course. Students will also be able to develop effective audit strategies. There are many complexities in understanding the payment process that may affect the findings discovered during the audit. Students will be walked through the chaos to better understand issues and document the correct findings amount. This course will also review some of the most common myths and misconceptions about having a contract and auditing it. Being able to understand contracts and contract risks will be discussed so that students can more effectively understand what the wording means and how a simple word can change the entire intention. Consequently, students will learn what the correct word choice should be and why the contract may not be as strong as they first imagined. Lastly, students will understand what is typically found during an audit and why the audit is important. They can bring this knowledge back to the audit committee or senior management to become a champion that will encourage further audits and to better protect the organization.

Core Topics:

- Project Types
- Project Life Cycle
- Auditing Payments
- Insurance
- Special Considerations

Auditing Corporate Culture

Prerequisite: Fundamentals of Internal Auditing (OAG101)

Advanced Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Internal auditors looking for techniques to audit an organization's culture and understand the related risks and vulnerabilities.

On-demand Learning Type: Skills

CPE: 6 – Enterprise only

Overview: This course provides internal auditors with a foundation for approaching an audit of company culture. Learners will be exposed to key drivers and frameworks that can help establish guidelines and parameters around the somewhat nebulous topic of culture. This course will prepare internal auditors for performing an audit of culture by first exposing them to ways in which an organization can be assessed.

We will review how attitudes towards risk, organizational strategies and values, structure, communication styles, and decision-making processes all factor into assessing organizational stances of culture. We will also explore considerations that auditors should be aware of when preparing to perform an audit of culture. Learners will leave this course with a better understanding of how to factor these considerations into their audit work and execute their audit engagement. Finally, this course will illustrate how to best perform an audit of culture and share the audit report with key stakeholders to yield improved outcomes for employees and organizational leaders.

Core Topics:

- Foundational Elements
- Assessing the Organization
- Considerations
- Performing the Audit

Communication Skills in Audit

Prerequisite: Fundamentals of Internal Auditing (OAG101)

Advanced Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Internal auditors of all levels seeking to improve their soft skills of effective communication, dealing with different personality types, and time management.

On-demand Learning Type: Skills

CPE: 4 - Enterprise only

Overview: As auditors, communication is an integral soft skill that must be honed. This course is intended to provide internal auditors of all experience levels with the tools and techniques used to improve communication and identify communication missteps. We will begin with an overview of communication channels, styles, and their purpose. With this foundation, we will determine which channel is most appropriate given different situations — a discerning communicator is an effective communicator! It is vital that auditors familiarize themselves with the array of communication tools they have at their disposal. This course will review these tools and provide learners with guidance as to when and how to use them effectively. By learning to become agile and adaptable, learners can become more tactical and specific in their communication strategies.

Core Topics:

- Communication Types Overview
- Dimensions of Communication
- Avenues and Artifacts

Risk Audit School

Prerequisite: Fundamentals of Internal Auditing or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal and External Auditors, Risk Management Specialists, and those charged with corporate governance responsibilities

CPE: 32

Overview: This course introduces participants to the basic concepts of risk, types of risks, and risk management (ERM) frameworks such as ISO 3000 and COSO ERM, and the IIA's professional guidance on risk management. It also covers how to conduct risk assessments and ways of reviewing several common types of functional risk assessments, such as a fraud risk assessment, an IT risk assessment, a financial risk assessment, and best practices. The course includes examples of tools, templates, and reports commonly used in the risk management process. Also covered are risk appetite, measuring the impact/likelihood or risks, and black swans.

The course then transitions to risk-based auditing and applies it toward developing the annual audit plan and planning at the engagement and audit program levels. Other topics include talent management strategies for risk-based auditing, root cause analysis, risk mitigation strategies, data analysis, and continuous monitoring tools to ensure there is an effective method for addressing risk.

The course also covers key business risks, including operational, strategic, people, regulatory and financial, cybersecurity, and culture, in addition to emerging risks. Participants will review articles, case studies, examples of tools and templates, and graphical depictions to help the student apply concepts and theories to practical use in their organization.

Core Topics:

- Risk Basics
- Enterprise Risk
- Enterprise Risk Management (ERM)
- Risk-Based Auditing
- Risk-Based Tools
- Key Business Risks
- Executive Perspectives on Top Risks
- Preparing IA Departments for Risk-based Auditing
- Marketing Risk-Based Auditing

Auditing for In-Charge Auditors

Prerequisite: Fundamentals of Internal Auditing or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Financial, Operational, Information Technology, and External Auditors

CPE: 24

Overview: This course focuses on how In-Charge Auditors lead audits. Participants will review audit program development and changes, risk assessments, setting and managing priorities, expectations, delegation, staff performance, and overall productivity, reviewing workpapers, stakeholder management, and incorporating fraud detection techniques into audit programs. The focus is on managing the dynamics of an audit and applying project management principles to increase the effectiveness of the engagement.

Core Topics:

- Overview
- Control Environment
- Audit Process
- Fieldwork and Program Development
- Risk Assessment Strategies
- Fraud Awareness
- Communication
- Marketing Internal Audit
- Audit Project Management
- Productivity

Better, Faster, Cheaper: Streamlining Your Internal Audit

Prerequisite: Fundamentals of Internal Auditing or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal Auditors, Compliance Experts, and leaders in Internal Audit departments

CPE: 24

Overview: An effective audit will produce the desired or intended result. It is built on a broad and deep assessment of an area, process, or system. It "begins with the end in mind" and creates a meaningful plan an auditor or audit team will follow. An efficient audit is one where we work productively with minimum wasted effort or expense. Audit leadership sets in motion themes and expectations based on risk assessment and communication with stakeholders inside and outside internal audit. Effective auditing means having a firm grasp of the scope, budget, resources, personnel, and timeline dedicated to a project. Auditors need to be able to manage unplanned issues while moving forward on audit goals and tasks in progress. An efficient audit requires focus and discipline to stay the course. This course explains and provides examples of who, what, why, and how to structure and manage a more in-depth and meaningful process and produce great results for both the client and auditor.

Core Topics:

- Preliminary Planning
- Initial Schedule
- Opening Stand-Up
- Initial Research
- Walkthroughs
- Risk Assessment
- Risks, Control Objectives, and Control Activities
- Iterations
- Refining Scope and Performance Measures
- Managing Oneself and the Team
- Analyzing Audit Quality Requirements
- Managing Fieldwork
- Written Communication
- Closing the Audit
- Following Up on Corrective Actions

Innovation for Internal Auditors

Prerequisite: Fundamentals of Internal Auditing or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal Auditors, Compliance Professionals, and leaders in Internal Audit departments who want to develop new audit approaches, expand current skills, re-energize the focus of audit activities, and who want to learn tips, tools, and techniques to embed innovation in their Internal Audit methodology

CPE: 24

Overview: The amount, speed, and impact of change have accelerated significantly, and all indicators point to more change in the future. Organizations are expected to innovate and become creative in pursuing business objectives, managing risks, and implementing appropriate controls that increase the likelihood of short-term and longer-term success. Internal Auditors must understand the dynamics driving these changes, how innovation is being used in modern organizations, and how it affects the efforts to provide reasonable assurance to the Board of Directors, management, and other stakeholders. Internal audit must understand change and innovation and embrace, adopt, thrive with it, and promote it. This course shows participants where and how innovation can work in their organization's favor, protecting and enhancing value while risks are appropriately managed. Internal audit must understand change and innovation and embrace, adopt, and promote it. Part one of this two-part series of courses will explore where and how innovation can work in the planning and execution of audit assignments to enhance and protect value while risks are managed.

Core Topics:

- Definition of Internal Audit
- The Role of Innovation in Internal Audit
- Improving Agility
- Embracing Innovation
- Risk Assessments
- Innovation and GRC
- Audit Plan Development
- Planning
- Fieldwork
- Reporting
- Follow-Up

Innovation for Audit Managers

Prerequisite: Fundamentals of Internal Auditing or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Audit Managers, Compliance Experts, and leaders in Internal Audit departments who want to develop new audit approaches, expand current skills, re-energize the focus of audit activities, and who want to learn tips, tools, and techniques to embed innovation in their Internal Audit methodology

CPE: 16

Overview: Managers must understand, deploy, and sustain innovation as a key characteristic of their units. This course shows how to embed innovation and agility in a department's methodology and administration, key considerations when implementing change initiatives, and techniques to successfully apply the Three Lines Model to provide integrated assurance. It also covers ways to make Internal Audit a more visible contributor to an organization's value protection and creation infrastructure.

Core Topics:

- Overview
- Change Enablement
- Strengthening the Evidence We Obtain and Use
- Expanding Our Role
- Management and Leadership in Internal Audit
- People, Processes, and Tools
- Achieving a Higher Level of Thinking
- Three Lines Model

Developing the Annual Audit Plan

Prerequisite: Auditing for In-Charge Auditors or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal Audit Managers and Directors, Audit Committee members, and External Auditors

CPE: 16

Overview: The course will prepare participants for developing the Internal Audit plan. Participants will assess applicable auditing standards for planning requirements while developing the technical and soft skills required to document and communicate the audit plan to clients and stakeholders. Participants will develop the skills necessary to identify internal, external, and industry risks. This course will focus on teaching participants how to assess resource requirements, identify potential audit projects, and align audit work to organizational risks. This course will prepare participants to build an audit plan aligned with organizational risks and communicate the plan and subsequent updates to stakeholders.

Core Topics:

- What Is the Standard?
- Understanding Your Industry
- Know Your Organization
- Identify a Risk Assessment Methodology
- Define Your Risk Universe
- Coordinate With Others
- Assess Your Resources
- Communicate the Plan
- Execute and Update

Risk Assessment Using Data Analytics

Prerequisite: Fundamentals of Internal Auditing, Risk School, or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal Auditors, Compliance Experts, and leaders in Internal Audit departments

CPE: 32

Overview: This course covers the basic concepts of risk assessments and enterprise risk assessments (ERAs) and how data analytics can optimize the risk assessment process; it also covers how to use risk assessments in risk-based auditing at the annual audit planning, the engagement planning, and the audit program development levels. It also includes Enterprise Risk Management (ERM) fundamentals, best practices, and examples of tools, templates, and reports commonly used in the risk management process. There is also coverage of ERM metrics using data analytics.

To better partner with key business stakeholders and add value to one's organization, it is necessary to understand key business risks. Therefore, the course devotes significant coverage to common business functions and their respective key processes, as well as the related risks, including Accounting, Financial Reporting, Human Resources, Legal, Sales, Contracts, Customer Service, Transportation/Delivery Service, IT, Manufacturing, Compliance, Quality Assurance, and Research & Development.

Throughout the course, there are exercises, informative articles, case studies, examples of tools and templates, and graphical depictions to help the participant apply concepts and theories to practical use in their organization. The course wraps up with reporting risk information to key stakeholders, including what's important to the Board as it relates to communicating risk information.

Core Topics:

- Enterprise Risks
- Enterprise Risk Management (ERM)
- Risk-Based Auditing
- Data Analytics
- Executive Perspectives on Top Risks
- Business Function Risk Assessment
- Culture Risk Assessment
- Risk Assessment Reporting

Intermediate IT Audit School

Prerequisite: IT Audit School or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Senior IT Auditors, Technologists, and Information Security Managers and Analysts with 2+ years of experience looking to increase their ability to move into a position of IT audit leadership

CPE: 32

Overview: An IT auditor with the skills, knowledge, and competencies to help organizations navigate the complex environment of IT risks has never been in higher demand. Every organization in every industry has become aware of the importance of proactively identifying, evaluating, and monitoring IT risks.

This course will reinforce and enhance the principles of assessing IT risks. Participants will examine ways to incorporate and implement the elements of risk assessment and audit planning; identify and apply pertinent audit and security resources; utilize tools of evaluating logical security; evaluate risks within database management systems; monitor risks within change management; test network perimeter security and cloud computing; evaluate threats within the internet of things, and add value in the IT auditor's organization regarding business continuity and disaster recovery planning and IT governance. The participant will also emerge with increased skills regarding effective communication and presentation of the results of the IT audit to various levels of leadership within the organization. The participant will be engaged through case studies of real-life examples and scenarios and acquire a wealth of resources, templates, and guides that can be adapted to and incorporated into any industry.

Core Topics:

- Risk Assessment and Audit Planning
- Audit and Security Resources
- Logical Security
- Database Management Systems (DBMS)
- Change Management
- Network Perimeter Security
- Cloud Computing
- Internet of Things (IoT)
- Business Continuity and Disaster Recovery Planning
- IT Governance
- Organization and Presentation of Information

Internal Audit Quality Assurance

Prerequisite: Auditing for In-Charge Auditors, Managing the Internal Audit Department, or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Chief Audit Executives who need to have a peer review conducted, as well as Internal Auditors who are asked to participate in conducting an external peer review. Participants should have 2-3 years of experience in performing audit reviews. For Chief Audit Executives attending this course, 4-5 years of supervisory/managerial-level experience is preferred.

CPE: 8

Overview: The International Standards for the Professional Practice of Internal Auditing (the Standards) require 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 course will explain how to conduct a self-assessment as outlined by the IIA Standards.

This seminar will cover what is mandatory and recommended in the International Professional Practices Framework (IPPF) and provide attendees with what they need to know to prepare for and undergo an external quality assessment review.

Attendees will understand how a QAR can benefit the internal audit activity, learn about the various review methodologies available, and discuss the important decisions that arise when preparing an internal audit department for a review.

Core Topics:

- Internal Audit Overview
- The Standards
- Methodology Resources
- The Review Process

Cybersecurity Audit School

Prerequisite: Introduction to Information Security or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Auditors and IT professionals seeking a foundational understanding of cybersecurity

CPE: 32

Overview: Today's auditor needs to know more than just the terms and concepts regarding cybersecurity. They need to understand what controls are needed, why they are important, where the controls should be positioned, and how to perform substantive tests to assess the control's reasonable effectiveness specifically related to cybersecurity. This class will explore cybersecurity through a series of lecture segments and related scenarios based on actual events designed to reinforce the attendee's knowledge of effective control design, execution, warning signs, and investigative techniques. By the end of the session, attendees will be armed with additional knowledge of how to implement and assess controls and how, as auditors, they can be valued players in their organization's "Cyber Defense Team."

Organizations need to establish robust cybersecurity programs to address risks to organizational infrastructure and data from cyberattacks through effective control design, the establishment of protection measures, the identification of warning signs, and investigative techniques. They also need to establish compliance with industry standards and regulatory requirements. This course will help you support your organization's cybersecurity objectives.

Core Topics:

- Cybersecurity Overview
- Asset Management
- Cybersecurity Protection Techniques
- Encryption, Digital Signatures, and Data Protection
- Event Detection, Incident Response, and Recovery
- Auditing Cybersecurity
- Audit Evidence and Reporting
- Course Wrap-Up

DevOps, DevSecOps, and Audit

Prerequisite: Introduction to Information Security or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal Auditors seeking to adopt a DevSecOps culture and employ a DevSecOps methodology into current business practices

CPE: 16

Overview: Organizations are increasingly adopting Development Security Operations (DevSecOps) as an evolutionary extension of Agile principles.

DevSecOps emphasizes communication and collaboration between development, security, and IT operations, building on Agile and Lean thinking to provide technology faster, with greater stability, quality, scalability, and security. The "Dev" side incorporates developers, front-end designers, and quality assurance. The "Ops" area brings in system administrators and support teams responsible for the product after it's moved to production. The "Sec" area covers all the cybersecurity professionals responsible for system control, compliance, and secure applications.

This course covers tools used to automate historically manual tasks like code quality checks, execution of test scripts, deployments, and the impact on traditional controls, such as Separation of Duties. It also covers the human-centric aspects of the process and the related risks that should be considered.

This course examines the DevSecOps methodology, how and where auditors can find their footing, best practices that need to be at the forefront of business leaders' minds, and the key shifts in mindset that must occur for a seamless transition from manual transactions to automated process flows.

Core Topics:

- What Is DevOps?
- Where Do Audit and Risk Fit In?
- The DevOps Process
- What Does a DevOps Culture Look Like?
- DevOps Practices
- DevOps and the Cloud
- What Is DevSecOps?
- Best Practices for DevSecOps
- Where Do We Go from Here?

Fraud Prevention and Detection

Prerequisite: Psychology of Fraud or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Financial, Operational, IT, and External Auditors; Audit Managers; Corporate Attorneys; Information Security professionals; Risk Management personnel and Line Managers who need to gain an understanding of how to successfully mitigate fraud risk in their organizations

CPE: 16

Overview: This course provides techniques to prevent and mitigate fraud within core business systems. After defining fraud and establishing the universal scope of the problem fraud presents to organizations worldwide, participants will explore the major schemes used to defraud organizations and individuals. In addition, understanding the psychology and motivations of fraudsters will help participants understand and develop strategies for prevention and detection.

This course covers how to create fraud risk statements, assess fraud risk, and create the right internal controls for your organization. By understanding the fraud risk universe facing organizations and the natural vulnerabilities that exist in their internal controls, participants will be better able to design fraud prevention, detection, and deterrence controls. There is also coverage of fraud analysis and investigations.

Other topics covered include techniques of fraud risk assessment, continuous monitoring, and key internal controls. Armed with a thorough understanding of how fraud occurs in disbursements, procurement, and payroll, participants will leave this course prepared with the knowledge needed to create an effective anti-fraud internal control environment.

Core Topics:

- Overview and Introduction
- Major Categories of Fraud
- Various Strategic Responses to Fraud Risk
- The Fraud Risk Structure
- Fraud Prevention Strategies and Techniques
- Strategies for Detecting and Deterring Fraud
- Fraud Risk Assessment
- Fraud Risk Mitigation in Disbursements
- Fraud Risk Mitigation in Procurement
- Fraud Risk Mitigation in Payroll

Methods in Audit Data Analytics

Prerequisite: Fundamentals of Internal Auditing or equivalent experience.

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Compliance Officers, Audit Managers and Directors, Financial, Operational, and IT Auditors, and key operational personnel

CPE: 24

AuditPro: Yes

Overview: In this course, participants examine real-world case studies demonstrating how various techniques are used to detect fraud, misuse, inefficiencies, and recover funds. The course covers data integrity, data quality, and data integration, will familiarize learners with identifying structured vs. unstructured data, intersecting data, and developing a systematic process of analysis. Learners will learn how to efficiently extract business insights from data, visually communicate those insights to their stakeholders, and apply these techniques to audit plans, tests, and other audit components. The course introduces learners to artificial intelligence, machine learning, the rise of quantum computing, and how these will impact the future of auditing.

Core Topics:

- Introducing Case Studies for Data Analysis
- Using Mind-Mapping Techniques to Discover Data Sources
- Normalizing and Forming Data
- Human Resources Data
- Website Analysis
- Analyzing AP Data
- Creating the Future of Audit Data Analytics

Data Mining for Auditors

Prerequisite: Fundamentals of Internal Auditing, Risk School, or equivalent experience

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Compliance Officers, Audit Managers and Directors, Financial, Operational, and IT Auditors, and key operational personnel

CPE: 24

Overview: This course will provide Internal Auditors with foundational and practical knowledge of data analytics and mining. This course is designed to differentiate these two concepts while providing auditors with tools to increase audit effectiveness. This course covers data mining techniques, maximizing data, data methodologies, and trend analysis. Participants will also identify ways to improve their continuous audit process and enhance outcome reporting through dashboard visualizations.

Note: Participants are encouraged to bring a laptop to perform several hands-on exercises involving data and how it should be applied to their organization.

Core Topics:

- Define Data Mining and Continuous Auditing
- Maximizing the Use of Data
- Data Methodologies
- Defining a Continuous Audit Process
- Report Outcome Focus

Forensic Auditing

Prerequisite: Fraud Prevention and Detection or equivalent experience.

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Financial, Operational, IT, and External Auditors; Audit Managers; Corporate Attorneys; Information Security professionals, and Risk Management and Human Resources personnel who need to gain an understanding of how fraud investigations are conducted and how to better collaborate with investigators

CPE: 16

Overview: This course provides an overview of forensic auditor duties and responsibilities applicable to various engagements in civil and criminal cases. It includes practical tools for the participant to identify applicable standards of performance, determine whether they can accept the case, and perform the engagement according to the requirements of the profession.

The course explains the strategy of planning and performing a forensic audit examination, inclusive of staffing and budgeting, and engagement letter requirements.
It reviews the evidence types, approaches to gathering and evaluating evidence, and best techniques for interviewing relevant parties. This course covers report writing and case presentations for internal and external use and will provide advice on testifying as an expert witness in a civil or criminal case.

Core Topics:

- Forensic Audit
- Engagement and Planning
- Investigation and Evidence
- Report Writing and Presentation
- Expert Witness

ACL Galvanized Diligent Scripting

Prerequisite: None

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Elementary scripters attempting to develop their starting scripts to support an audit department with individuals who will perform their own analyses. This course will also benefit scripters who are looking to develop and generate multi-use scripts to feed other users' data, which will be used for other analyses. Individuals taking this course should have 0-2 years of experience in scripting environments.

On-demand Learning Type: Skills

CPE: 8 – Enterprise only

Overview: This course is intended to help scripters support internal audit departments and improve their testing processes, and reviews the scripting process from planning to development to interactivity and export. Participants will review the basics of data mining, including how data mining can be used to support audit initiatives. Participants will also work to hone their decision-making skills with respect to data mining and assess how audit objectives align with the data mining process.

This course covers topics associated with script planning, including file formats, file import naming conventions, import types, and associated file clean-up. Once planning is complete, this course reviews files and commands that can improve script development and efficiency. Finally, participants will review different methods and best practices for improving script interactivity, including variables, date ranges, filters, and operators. The course includes several live demonstrations that directly correlate to real-world scenarios that scripters and Internal Auditors will face in the field.

Core Topics:

- Planning Your Data Mining Script
- Developing Your Data Mining Script
- Making Your Scripts Interactive

ESG Audit

(Environmental, Social, and Governance)

Prerequisite: Fundamentals of Internal Auditing (OAG101)

Advanced Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: All business professionals interested in learning the key ESG factors and how they can be integrated into a company's internal audit and financial reporting processes.

CPE: 8

Overview: This course will provide business professionals with a historical background on how these Environmental, Social, and Governance (ESG) factors evolved and how they play an important part in a company's current financial reporting and corporate disclosures. We will look at the current landscape of recommended ESG reporting standards outlined by various organizations and how you can leverage them to create your own set of policies and controls for ESC reporting and disclosures. Finally, we will also look at ESG from an investor's and consumer's perspective and give an overview of how companies are positioning their ESG reporting in alignment with their investments, interests, and values.

Core Topics:

- The Evolution of ESG
- What Is ESG?
- ESG Considerations
- Financial Reporting Requirements
- Audit Reporting Requirements
- How to Evaluate Corporate Performance
- Investor and Consumer Perspectives

Internal Audit School

Prerequisite: Fundamentals of Internal Auditing, Auditing for In-Charge Auditors, or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Internal and External Auditors, Risk and Compliance professionals, and IT Auditors who require a comprehensive approach to operational audits of core business functions

CPE: 32

Overview: Participants will build on the fundamentals of modern internal auditing and practice how to conduct operational audits and develop audit programs for auditing business processes, including Purchasing, Contracting, Vendor Selection, Marketing, Sales, Human Resources, IT general controls, management, and accounting functions like Accounts Payable, Accounts Receivable, Inventory, Payroll, Treasury, and Fixed Assets.

Core Topics:

- Key Elements of Operational Auditing
- Components of Operations Auditing
- Auditing Purchasing and Contracts
- Auditing Marketing and Sales
- Auditing Human Resources
- Auditing Finance, Treasury, and Accounting
- Auditing Information Technology
- Auditing Supply Chain
- Auditing Management and Corporate Governance
- The Future of Operational Auditing

Fraud Data Analytics

Prerequisite: Testing for Occupational Fraud, Forensic Auditing, or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

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.

CPE: 24

Overview: Fraud data analytics is the process that allows the auditor/investigator to evaluate the entire set of data to identify fraud red flags, which are related to a specific fraud scenario; they will then alert the auditor/investigator to focus on certain transactions and areas to review controls, conduct interviews, and examine source documents to determine whether a fraud scheme is occurring or there is simply an error or mistake. Thus, fraud data analytics aims not to identify fraud but rather to identify red flags that would assist the auditor/investigator generate a sample of transactions to examine further in detail. Fraud data analytics does not replace the "old fashion" audit and investigative procedures of gathering relevant and sufficient evidence to conclude whether a fraud scheme has been perpetrated.

Core Topics:

- What Is Fraud Data Analytics?
- Fraud Data Analytics Program
- Cultivating Additional Skills
- Travel and Entertainment
- Payroll
- Credit Cards and P-Cards
- Accounts Payable and Disbursement
- Shell Companies
- Procurement
- Anti-Bribery and Corruption (ABC)
- Findings and Value
- Financial Statements, Journal Entries, Revenue, and Liabilities

Governance, Risk, and Compliance (GRC)

Prerequisite: Advanced Auditing for In-Charge Auditors, Managing the Internal Audit Department, or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Chief Compliance Officers, Chief Audit Executives, Audit Directors and Managers; Chief Risk Officers and Chief Ethics Officers; Internal and External Auditors, and anyone with GRC responsibilities

CPE: 24

Overview: This course provides a roadmap to develop, implement and sustain an integrated GRC infrastructure to help participants implement and maintain a GRC framework. Many organizations have implemented selected components of a GRC framework, but the challenge remains to integrate the disparate components. Those attending this course will examine ways of building, sustaining, and reviewing GRC programs.

Core Topics:

- Overview
- COSO Internal Control Framework
- COSO Enterprise Risk Management Framework
- Effective Compliance and Ethics Programs
- GRC Overview
- GRC Capability Model Element View
- Element 1 – Learn
- Element 2 – Align
- Element 3 – Perform
- Element 4 – Review
- Wrap up

Auditing the Enterprise Risk Management (ERM) Process

Prerequisite: Risk Audit School (OAR201) or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Audit Directors and Managers, Risk Officers, Internal and External Auditors, Information Technology Auditors, and Operations Managers

CPE: 16

Overview: This course provides an overview of the Enterprise Risk Management (ERM) process and all the underlying elements of ERM, including risk appetite, governance, and roles and responsibilities. The course includes the attributes that make an ERM process effective, such as addressing black swans, using risk-driven metrics, and linking ERM with the organization's strategy. Most of the course will involve methods for auditing the ERM process by assessing the process according to the COSO framework, comprising five components and twenty principles.

The course also includes ISO 31000, a summary of key highlights, and a comparison of the commonalities and differences between the ISO risk management framework and the COSO risk management framework.

The course also covers the application of concepts using examples, case studies, exercises, and ERM reporting to various stakeholders.

Core Topics:

- Enterprise Risk Management (ERM)
- COSO Principles 1-20
- ISO
- Reports

Testing for Occupational Fraud

Prerequisite: Fundamentals of Internal Auditing, Fraud Prevention and Detection, or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Auditors, Investigators, and Compliance Officers

CPE: 8

Overview: This course provides the basic knowledge needed to understand and identify different types of occupational fraud that may exist in organizations.

Core Topics:

- Fraud Basics
- Corruption
- Asset Misappropriation
- Financial Statement Fraud

Using Risk Assessment to Build Individual Audit Programs

Prerequisite: Risk School, Risk Assessment of Business Functions Using Data Analytics, or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Financial, Operational, Business, and IT Auditors interested in broadening their knowledge of risk assessment techniques and principles

CPE: 24

Overview: In this course, participants will learn how to use risk assessment techniques and principles to build and conduct risk-based and value-added audit programs. It explores progressive approaches to assessing risk and determining the most appropriate strategies to build targeted audit programs for organizations and audit units. Attendees will learn how to build audit programs that will encompass an evaluation of a wider spectrum of risks: financial, information systems, regulatory and compliance, human resources, health & safety, operational effectiveness and efficiency, and reputational risks.

Through case studies and other interactive approaches, participants will have an opportunity to be hands-on in working through various scenarios. Finally, participants will learn effective approaches to include sustainable risk-mitigation and corrective action strategies in the report and ongoing monitoring efforts. Attendees will emerge from this course with a toolbox of proven implementable approaches that will enhance any internal audit function to generate high-value and high-impact outcomes.

Core Topics:

- What Is Risk Assessment?
- Strategic Plans
- Organization's Risk Assessment Approach
- Assessing Risk
- Categorization of Risks
- Using Data Analytics
- Risk-Based Audit Programs
- Risk-Based Audit Reports
- Corrective Action Plans
- Updating Risk Assessments

NIST Cybersecurity Framework

Prerequisite: Introduction to Information Security and Cybersecurity Audit School or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Information Security and Network professionals, Chief Data Officers, Chief Information Security Officers, and Senior IT Auditors wanting to gain a deep understanding of the Cybersecurity Management System Framework

CPE: 32

Overview: NIST is the de-facto standard for security, compliance, and privacy in the US. One must comply with NIST standards if/when doing business with the US federal government, managing critical infrastructure, or maintaining personally identifiable information (PII).

NIST provides the Cybersecurity Framework (CSF) and Risk Management Framework (RMF) to guide organizations in securing their infrastructure, systems, and data. In this course, participants will apply the NIST Cybersecurity and Risk Management Frameworks to better protect their infrastructure, detect possible cyber incidents, and appropriately respond and recover should they occur. We teach participants how to become well-versed in the NIST CSF and RMF, how to implement them, and ways to effectively manage CSF and RMF processes for optimal security, privacy, and compliance.

Core Topics:

- NIST Cybersecurity Overview
- NIST CSF Identify
- NIST CSF Protect Function
- NIST CSF Detect Function
- NIST CSF Respond Function
- NIST CSF Recover Function
- NIST RMF Preparation
- NIST RMF Categorization
- NIST RMF Control Selection
- NIST RMF Control Implementation
- NIST RMF Control Assessment
- NIST RMF Authorization
- NIST RMF Risk Monitoring
- Overviews

Managing the Internal Audit Department

Prerequisite: Auditing for In-Charge Auditors or equivalent experience

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Internal Audit Managers, Directors, and Supervisors

CPE: 24

Overview: This course provides guidance and standards from the IIA for audit professionals and effective ways of conducting audits, from the audit plan to engagement planning as well as execution and audit reporting. These concepts are complemented with innovative tools and methodologies, including data analytics, agile auditing, and GRC software for more efficient and effective audits that add value. In addition to best practices for technical skills for auditors, it also covers soft skills that are critical for an audit leader's success, including best practices in project management, communication skills, conflict management, and leading with empathy.

The course addresses the challenging pursuit of Internal Audit, becoming strategic partners, and having a seat at the table. Additionally, there is coverage on how audit leaders can play a role and add value in several common strategic initiatives related to risk management (ERM), corporate culture, IT, operations, and others. Finally, the course wraps up with how best to communicate with and report to the Board and the Audit Committee, whether the participant attends Board meetings or is involved with providing input into Board reporting. These concepts will be reinforced with exercises and case studies throughout the course to allow participants to apply what they have learned using real-world examples and situations.

Core Topics:

- Governance
- The IA Department
- Audit Talent Management
- The Audit Plan
- Audit Engagements
- Audit Tools and Methodologies
- Audit Leadership Skills
- Strategic Partners
- Audit Committee and the Board

Certified Information Systems Security Professional - CISSP 2021

Prerequisite: CompTIA Network+ and Security+ certifications or equivalent experience are highly recommended.

Advanced Prep: At least five years of professional experience in two or more fields related to the Common Body of Knowledge (CBK) security domains. Earning a four-year college degree will satisfy one year of the required experience.

Field: Auditing

Who Should Attend: Experienced IT security practitioners, auditors, consultants, investigators, network or security analysts and engineers, network administrators, information security specialists, and risk management professionals.

Learning Style: On-demand only

Learning Type: Certification prep

Level: Advanced

Overview: The Certified Information Systems Security Professional (CISSP) certification is the gold standard in the IT Security field. Security professionals that have achieved their CISSP designation are regarded as some of the most talented and knowledgeable people in their field. The certification demonstrates that the holder has been working in IT Security for over five years, has a broad range of knowledge in the domains related to creating, supporting and maintaining a secure IT infrastructure, and can implement things like risk management and risk identification.

Core Topics:

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security
- The CISSP Toolbox

Systems Security Certified Practitioner SSCP (2022)

Prerequisite: CompTIA Network+ and Security+ certifications or equivalent experience are highly recommended.

Advanced Prep: At least one year of work experience in one or more of the domains of the SSCP Common Body of Knowledge (CBK).

Field: Auditing

Who Should Attend: IT Administrators, managers, directors and network security professionals, auditors, consultants, investigators and risk management professionals.

Learning Style: On-demand only

Learning Type: Certification prep

Overview: The Systems Security Certified Practitioner (SSCP) is ideal for IT administrators, managers, directors and network security professionals responsible for the hands-on operational security of their organization's critical assets. The certification demonstrates that the holder has been working in IT Security for at least one year, has a broad range of knowledge in the domains related to creating, supporting, and maintaining a secure IT infrastructure, and can implement, monitor and administer things like risk identification, risk management, best practices, policies and procedures.

Core Topics

- Security Operations and Administration
- Access Controls
- Risk Identification, Monitoring & Analysis
- Incident Response and Recovery
- Cryptography
- Network and Communications Security
- Systems and Application Security
- The SSCP Toolbox

Enterprise Solutions

Fundamentals of Auditing Process Automation

Prerequisite: None

Advance Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Auditors, Information Security, and Risk professionals wanting to gain a general understanding of process automation and how to assess Business Process Management (BPM), Robotic Process Automation (RPA), applications, and servers

CPE: 24

Learning Style: Enterprise only

Overview: This course provides an introduction to software automation technologies and key considerations for organizations getting started on their automation journeys. Key areas covered include different types of process automation from industrial, to IT (DevOPs) and digital transformation made possible through robotic process automation (RPA) and cognitive automation using artificial intelligence (AI). The course discusses the role Business Process Management (BPM), process workflows and governance play when considering these technologies and how to implement and assess them.

Core Topics:

- Automation Explained
- Governance and Management
- Automation Strategy and Program
- Ethics of Automation and Artificial Intelligence
- Common Automation Workflows: Understanding Workflows
- Tips for Assessing Automation

Essential Interpersonal and Team Building Skills for Auditors

Prerequisite: None

Advance Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Financial, Operational, and IT Internal Auditors

CPE: 16

Learning Style: Enterprise only

Overview: This course shows how to build teamwork, communicate effectively, deal with difficult people, anticipate misunderstandings, enhance your emotional intelligence, ways to leverage critical thinking in decision-making, enable change, and work effectively with others. This course also introduces tools to improve your audit projects and time management and provides best practices for building a team that works cohesively towards the same end goal.

Core Topics:

- The Effective Auditor
- Team-Building
- Next Steps

IT Risk Management

Prerequisite: None

Advance Preparation: None

Learning Level: Entry-level

Field: Auditing

Who Should Attend: Information Security, IT Audit, and Audit professionals looking to gain greater knowledge on performing an IT risk assessment and developing a strong IT risk management program

CPE: 24

Learning Style: Enterprise only

Overview: This course covers risk management, the primary process organizations use to determine their capability to identify, manage, and respond to risk and verify their ability to maintain confidentiality, integrity, and availability of their information assets. Participants review common risk assessments and analysis requirements for meeting both regulatory and industry expectations and ways to demonstrate technology risks, and their potential outcomes are embedded in their risk management process.

Core Topics:

- Introduction to Risk Management
- IT Risk Identification and Risk Universe
- Risk Scenario Development
- Risk Analysis
- Risk Evaluation
- Business Impact Analysis Overview
- Risk Response
- Cost Benefit Analysis and Business Case
- Control Development
- Risk Monitoring and Reporting

IT Auditing and Controls

Prerequisite: None

Advanced Preparation: None

Learning Level: Entry-Level

Field: Auditing

Who Should Attend: Internal Audit Staff, Seniors, and Managers responsible for performing integrated internal audits or those who want an introduction to IT auditing

CPE: 24

Learning Style: Enterprise only

Overview: Internal and Operational Auditors in today's complex organizations must understand information systems and be able to function within a technical environment. This course outlines the concepts of information technology to understand audit concerns in the IT environment. Participants will review critical business application system controls and the supporting IT general controls. The focus is on key risks and controls in critical areas like user access to business applications, database security, networks, change management, and disaster recovery.

Core Topics:

- Introduction to IT Risks and Controls
- Planning IT Audits
- Audit and Control Frameworks and Standards
- Basics of Information Technology
- Database Technology and Controls
- Network Technology and Controls
- IT Governance
- IT General Controls
- Business Application Controls

Oil, Gas, and Petrochemical Internal Audit College

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Internal and External Auditors, Compliance, and Risk Management professionals

CPE: 40

Learning Style: Enterprise only

Overview: This course is tailored specifically for oil, gas, and petrochemical companies and provides practical and valuable guidance on risk-based operational auditing. It teaches participants how to identify and prioritize the risks and assess the efficiency, effectiveness, and economics of both core and non-core business processes and provides practical exercises to help delegates gain confidence in the techniques presented and their ability to use them. Report writing is also explored to help delegates not only understand who Internal Audit's stakeholders are but to help delegates get their messages across clearly and concisely. Delegates are given the opportunity to provide examples from their workplace for review and discussion.

Since oil and gas relies on the need for outside experts, the course also covers the requirements for reporting on the opinions of others. It explores areas such as walkthrough contracts that are necessary and risky when it comes to oil and gas companies. It also examines how oil and gas companies can still be ESG compliant and stand out from the competition.

Core Topics:

- Setting the Scene – Internal Auditing Today
- Understanding Risk Management and Risk-Based Auditing
- Auditing the Procurement Function
- Auditing Inventory Management
- Auditing Major Contracts
- Auditing Turnaround (Shutdown) Contracts
- Auditing Governance and Ethics
- Auditing Health, Safety, and Environmental Management Systems
- Auditing Report Writing
- Auditing Projects
- Auditing Joint Ventures
- Auditing Outsourced Operations

Audit and Control of DevOps

Prerequisite: Intermediate IT Audit School (ITG214), Auditing Agile and Scrum Development Projects (ITG213), or equivalent experience

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: IT Auditors, Information Security professionals, Risk Managers, and those assigned to form or participate in a DevOps Governance Committee who wish to gain an understanding of how to govern, manage, and assess a DevOps environment

CPE: 16

Learning Style: Enterprise only

Overview: This course covers working collaboratively with business owners, developers, operations personnel, quality assurance, testers, security specialists, and suppliers to deliver software continuously and competitively. It covers continuous development, testing, deployment, monitoring, feedback, vulnerability scanning, and auditing of DevOps. Since this is a continuous process, the focus is on where to find the risks in a dynamic environment.

Core Topics:

- What Exactly Is DevOps?
- The DevOps Lifecycle
- Is It Development? Is It Operations? Is It Both?
- Top 10 DevOps Myths and Why They are Wrong
- Top 10 Problems That Cause DevOps to Fail and How to Spot Them
- Top 10 DevOps Controls
- Can the Cloud Be Part of the Solution?
- How to Audit DevOps
- Don't Trust the Interfaces
- Continuous Delivery: A New Type of Change Management
- Reporting Deficiencies

Auditing Agile and Scrum Development Projects

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Financial Auditors, IT Auditors, Application Systems Development team leaders, Scrum Masters, and project sponsors

CPE: 16

Learning Style: Enterprise only

Overview: This course covers Agile and Scrum methodologies, expectations, and business models and focuses on what auditors and developers must review and manage to facilitate rapid application systems development and project success. It includes considerations during the entire project lifecycle, highlighting the key risks and considerations auditors should keep in mind to protect organizations from project underperformance.

Core Topics:

- What Exactly Are Agile and Scrum?
- How to Learn About the Project in Time to Get Involved
- What Is the Definition of Success vs. Failure?
- The Infrastructure That Should Be in Place Before the Project Begins
- What to Look For Before the Project Begins
- The Project Manager
- The Steering Committee
- The Project Plan
- What to Look For During the Project and the Key Triggers to Apply
- Testing
- Interfaces
- Change Management
- Reporting Deficiencies

Information Security Boot Camp

Prerequisite: Introduction to Information Security (ISG101)

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: information security and IT managers; cybersecurity specialists; information security analysts; data analysts; system architects, system administrators; network administrators; IT auditors; audit management; consultants; compliance managers, and anyone needing a course on information security concepts and practices

CPE: 40

Learning Style: Enterprise only

Overview: This course covers the $(ISC)^2$ Common Body of Knowledge (CBK) and evaluates real world methods and tools required to construct or audit a comprehensive information security framework. It provides a business-oriented, architectural perspective that defines how to organize and oversee a risk-based enterprise information security program., blending theories and best management practices with key physical and information technology safeguards.

Key references and yardsticks are provided to gain familiarity with industry-leading practices, legislation, and professional standards for information/cyber security and audit practitioners.

The course also provides unit and course review exercises to help participants prepare for the CISSP exam (or similar such as CISA) and help guide their organization as it develops or revises its information security program. Multiple takeaways are provided.

Core Topics:

- Security and Risk Management
- Laws and Standards Affecting Information Security and IT Audit
- Security Engineering: Security Models, Mechanisms, and Architectures
- Network Security Concepts and Solutions
- Cryptography
- Identity Management/Access Controls
- Software Development and Application Security
- Asset Security: Physical, Human Resources, and Environment
- Availability: Data Recovery and Business Continuity Planning

Value for Money and Performance Auditing

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Chief Internal Auditors, Internal Audit Managers, Lead Auditors, and other experienced auditors in private, public, and non-profit practice

CPE: 24

Learning Style: Enterprise only

Overview: This course focuses on the three Es of performance auditing - economy, efficiency, and effectiveness of programs, projects, and processes - and provides ways to assess these themes within organizations.

Core Topics:

- Setting the Value for Money (VFM) Scene
- Context and Definitions
- The Three Es of VFM
- Developing a VFM Audit Program
- Readiness Check
- VFM Techniques
- Defining the Audit Questions
- Planning the VFM Audit
- Overview of the VFM Process
- Collection Plan
- Audit Completion
- VFM Audit Reporting

Information Management and CDMP Professional Certification

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Business Intelligence, Data Warehouse Developers and Architects, Data Modelers, Developers, Data Analysts, Business Analysts, Database Administrators, Project Managers, and IT Consultants

CPE: 40

Learning Style: Enterprise only

Overview: In this course, students prepare for the CDMP certification and review the relevant information disciplines and how information architecture is applied. The exam is taken on the last day of the course.

Core Topics:

- Business Intelligence, Data Warehouse Developers, and Architects
- Data Modelers
- Developers
- Data Architects and Analysts
- Enterprise Architects
- Solution Architects
- Application Architects
- Information Architects
- Business Analysts
- Database Administrators
- Project / Program Managers
- IT Consultants
- Data Governance Managers
- Data Quality Managers
- Information Quality Practitioners

COBIT 2019: Integrating COBIT into Your IT Audit Process

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Anyone responsible for implementing or assessing IT and security controls; Internal Audit Seniors, Managers, and Senior Managers involved with identifying, assessing, and reporting on technology-related risks

CPE: 24

Learning Style: Enterprise only

Overview: This course reviews the COBIT 2019 Framework and focuses on how this globally recognized framework can be used to evaluate IT activities' effectiveness. It explores the significant changes incorporated in the newest release that can be used in executing IT audits. It covers how to use COBIT 2019 in conjunction with other internationally recognized standards and frameworks.

Participants will be exposed to examples using COBIT 2019 to plan and execute audits for IT governance, risk management, security management, and business continuity. As a result of these exercises, participants will better understand how to use COBIT 2019 to provide a comprehensive and effective audit approach.

Core Topics:

- COBIT Background
- Summary of COBIT 2019
- International Security Standards and Frameworks
- Assessing IT Governance Using COBIT 2019
- Risk Management
- Security Management
- Manage Continuity
- Integrating the COBIT 2019 Process Capability Model
- COBIT Related Resources

Network Security Essentials

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

Advance Preparation: None

Learning Level: Intermediate

Field: Auditing

Who Should Attend: Information Security Professionals and IT Auditors working with networks

CPE: 24

Learning Style: Enterprise only

Overview: This course covers the basic operating characteristics and risks associated with LANs, WANs, client/server, and other forms of networking and distributed computing architectures. It includes best practices for securing and auditing network applications, interconnection devices and remote access, and perimeter security services.

Participants 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. The course also includes checklists at the end of each control-related section.

Core Topics:

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

Securing and Auditing Virtualized Environments

Prerequisite: Network Security Essentials (ASG203), Intermediate Audit School (ITG241), or equivalent experience

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

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

CPE: 40

Learning Style: Enterprise only

Overview: This course focuses on ESX and Hyper-V security. The course begins with virtualization basics, hardware virtualization considerations, and different versions of ESX. It examines best practices for securing ESX servers, access to the management console, ESX logging, and other configuration issues to ensure the ESX virtual server hosts are secure and stable. It then covers Hyper-V and best practices for securing a Hyper-V environment. It also covers the benefits and synergy of virtualization when implementing the organization's disaster recovery strategy. Participants tie these concepts together by formulating a suggested audit program of ESX/Hyper-V and the virtual server environment.

The course includes case studies using a combination of live demonstrations and exercises that reinforce important virtualization concepts and associated audit points addressed in real audit projects.

Core Topics:

- Virtualization Basics
- vSphere/ESXi Basics
- Hyper-V Basics
- Virtualization and Disaster Recovery
- Developing an Audit Program for ESX
- Minimum Items to Review in a Virtualization Audit
- ESX Case Study

Advanced IT Audit School

Prerequisite: Intermediate IT Audit School (ITG241), Network Security Essentials (ASG203), or equivalent experience

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: IT, Internal and External Auditors; IT Audit Managers, Information Security Managers, Analysts with 5+ years of experience, or those tasked with auditing web servers, application services, Database Management Systems, and enterprise architecture

CPE: 32

Learning Style: Enterprise only

Overview: This course covers the building blocks of IT audit and security, including identity and access management, web-based e-commerce application threats, vulnerabilities, and standards associated with privacy issues and intellectual property concerns. It places special emphasis on discovering best practices and standards for auditing web (HTTP) servers and application servers and enables participants to walk away with tools, techniques, and checklists for discovering and testing web and application server security.

It also covers auditing database management systems within the context of robust but practical enterprise architecture and governance models and reviews web services and service-oriented architectures, including SOAP, ReST, SOA, and ESB. Participants will also review safeguard concepts and best practices for secure mobile and wireless applications.

Core Topics:

- Identity and Access Control Management (I&ACM) Architecture
- Web Application Architectures
- Auditing Web (HTTP) Servers
- Secure Application Design, Testing, and Audit
- Auditing Application (Middleware) Servers
- Auditing Database Management Systems
- Web Services and Service Oriented Architectures (SOA)
- Mobile Application Security and Audit
- Laws and Standards Affecting IT Audit

Audit and Security for Cloud-Based Services

Prerequisite: Network Security Essentials (ASG203), Intermediate IT Audit School (ITG241), or equivalent experience

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Operational, Business Application, IT, and External Auditors; Audit Managers and Directors; Information Security professionals

CPE: 16

Learning Style: Enterprise only

Overview: This course covers the current state of cloud computing, its common architecture, and the major SaaS, PaaS, and IaaS providers in the market today. It covers the security and control deficiencies in cloud-based services and looks at Security as a Service as a way to protect against them. Participants review a risk-based approach to audit and controls for cloud-based services and investigate areas such as cloud-based network models, cloud access security brokers, disaster recovery, and governance in a cloud environment. It reinforces the concepts covered with examples to help participants identify the risks, controls, and gaps in cloud services.

Core Topics:

- Cloud-Based Computing: An Architectural Overview
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- Brokered Cloud Services
- Security as a Service
- Cloud-Based Security Standards and Dependencies
- Governance in a Cloud Services Environment
- Disaster Recovery in a Cloud-Based Environment
- Cloud Security and Audit

Securing and Auditing Windows Active Directory Domains

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

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: System and Security Administrators, InfoSec Managers And Analysts, Network Administrators, Security Architects, IT Auditors, and Consultants

CPE: 32

Learning Style: Enterprise only

Overview: This course focuses on the skills required to effectively audit Active Directory. Using a Cloud-based Lab, each participant will have their own virtualized Windows Server 2016 Domain Controller and Windows 10 Workstation to practice the concepts and techniques learned during the class with a series of 15 hands-on labs. Output from each of the labs will be incorporated into an Excel spreadsheet. This spreadsheet can be used as the basis for an audit program after the class is completed. Separate sheets in the Auditing Active Directory Excel Spreadsheet summarize how to obtain Active Directory data using PowerShell scripts, a place to store samples of the PowerShell output, and items to review in the output. Participants can email their completed spreadsheet to take with them after the class with lab notes and PowerShell Scripts. The course provides a practical methodology for auditing and securing Active Directory, attacks against Active Directory, and how to protect against those attacks. Audit techniques are designed to make Active Directory more secure and difficult to hack. The last day of class includes a role-playing exercise to put into practice the skills learned earlier in the course in a challenging real-world auditing environment.

Core Topics:

- Windows and Windows Networks
- Auditing Active Directory Core Components
- Auditing Active Directory Users
- Auditing Active Directory Groups
- Auditing Password Policies
- Auditing Folder Rights
- Auditing Active Directory Delegation
- Security Compliance Manager and Group Policy
- Auditing User Rights and Event Viewer Logs
- Hardening Active Directory
- Active Directory Case Study

Cybersecurity Risks from an Audit Manager's Perspective

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

Advance Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Internal Audit Seniors, Managers, and Senior Managers involved with identifying, assessing, and reporting on technology-related risks for their Internal Audit projects or the Internal Audit Risk Assessment

CPE: 16

Learning Style: Enterprise only

Overview: This course 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 ensure that IT risks are adequately addressed. The information is presented in straightforward language. The course provides participants with a comfortable working knowledge of IT terms and concepts and updates on new and emerging technologies affecting organizations. It also helps establish a strategic response to IT risks.

Core Topics:

- IT Risks
- Basics of Information Technology: Battling the Buzzwords
- Logical Security Risks and Controls
- Network Risks and Controls
- Database Risks and Controls
- IT General Controls
- Auditing System Development Projects
- Assessing IT Governance
- Audit and Control Frameworks and Standards

High-Impact Skills for Developing and Leading Your Audit Team

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

Advanced Preparation: None

Learning Level: Advanced

Field: Auditing

Who Should Attend: Internal Audit Seniors, Managers, and Directors with 5+ years of experience, and those responsible for the completion of multiple internal audit projects

CPE: 24

Learning Style: Enterprise only

Overview: This course covers leadership techniques that enhance the role of leaders, improve the performance of the audit team, and boost its profile in the organization. It looks at the participants' skills and helps them master strategies that allow them to leverage their audit knowledge with proven tactics that will inspire and motivate the staff.

It covers the essential practices of sound audit leadership, including modern goal-setting methods, effective coaching, establishing hiring practices that will attract the best people, leading a productive team and departmental meetings, and mastering the art of persuasion. Participants will gain insights into oral and written communication skills and new ways to help the team members reach their highest potential.

Core Topics:

- From Managing to Leading
- Essential Leadership and Management Skills
- Hiring and Motivating Employees
- Time, Stress, and Priorities Management
- Communication Skills, Team Building, and Conflict Management
- Common Management Mistakes
- Training and mentoring Programs
- Leading Change
- Global Auditing

CPE Program Presentation

Standard Terms

At ACI Learning, we are dedicated to assisting every student in getting trained, certified, employed, and on a path toward advancing in high-growth IT, cybersecurity, and auditing careers. The following guidelines have been implemented to maintain compliance with all education Boards (State and the VA) and help students progress toward obtaining skills, certifications, and employment.

Online Synchronous Learning Courses

ACI Learning records online synchronous courses for quality control, audit, and compliance purposes. Your consent to being recorded is established when you log into the course; the content of these recordings will not be shared with any outside entity.

Attendance Requirements

Students are expected to arrive on time for classes with the proper materials and attitude. An overall attendance rate of 100% is expected to fully absorb the materials and complete labs. If you have an expected absence, please email clientservices@acilearning.com or your instructor ahead of time. A minimum of 83% attendance is required to receive a Certificate of Completion. Any extended absence from class may result in reduced CPEs earned.

Conduct Policy

All students are expected to treat all staff, instructors, and students respectfully. Coming to class on time with all courseware and materials is crucial to success in your program. ACI Learning reserves the right to dismiss any student for language or gestures we deem offensive. No weapons, drugs, or smoking of any kind are allowed on any ACI Learning location and platform. During class, active participation is expected. Cell phones and sleeping during class are prohibited.

Reschedule Policy On-line Corporate Training Courses

You may elect to substitute another individual from the same company for the same seminar date and location without incurring any fees.

In-Person Client-Selected Locations and Virtual Training Programs Cancellation Policy

Cancellations can be made in person, by electronic mail, or by termination.

- A full refund will be made to any student who cancels the enrollment contract within 72 hours (until midnight of the third day, excluding Saturdays, Sundays, and legal holidays) or close of business the Thursday prior to commencement of class, whichever is sooner after the enrollment contract is signed.
- A full refund will also be made to any student who cancels enrollment three business days prior to scheduled class days, except that the school may retain not more than $100 in any administrative fees charged, as well as items of extra expense that are necessary for the portion of the program attended such as courseware and lab fees.

Virtual Training, Seminars, Webinars, and Courses

If you can no longer attend the seminar, please review the cancellation policy below and provide written notice to ACI Customer Service at provisioning@acilearning.com. Cancellations received 14 or more days prior to the event start date will be entitled to a full refund. If the course was purchased and registered for less than 14 days prior to the event start, it could be refunded within 24 hours of purchase, up until the start time of the class.

No refunds or transfers will be given for cancellations received 14 days or less prior to the event start date (the exception being the 24-hour cancellation option for late registrations less than 14 days prior).

Those who do not contact ACI Learning with written notice about their cancellation prior to the event date and those who do not attend the training are responsible for the full non-refundable, non-transferable tuition.

NASBA Courses and Seminars

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