RCI
Risenhoover Consulting, Inc.

Auditing Systems, Applications and the Cloud

July 14-18, 2025

8:00 am to 5:00 pm CDT Monday-Friday

Instructor: Clay Risenhoover, CPA.CITP, CISSP, CISA, CISM, CIA, CEH

Join us for RCI's popular IT audit course: **Auditing Systems, Applications and the Cloud**. This 5-day, 40 CPE course gives the student the tools, techniques and thought processes required to perform meaningful risk assessments and audits. Learn to use risk assessments to recommend which controls should be used and where they should be placed. Know which tools will help you focus your efforts and learn how to automate those tools for maximum effectiveness.
20 hands-on exercises plus bonus daily capstone labs.

Learning Objectives

- Day 1: Audit in the Enterprise and Cloud
  - Fundamentals of IT audit
  - How to gain visibility in the cloud
- Day 2: PowerShell, Windows System and Domain Auditing
  - Understanding PowerShell
  - Taking domain and system measurements
- Day 3: Auditing Linux
  - Unix security
  - Tools for measuring Linux security
- Day 4: Auditing Cloud Infrastructure
  - Testing virtualized systems and applications
  - Auditing cloud infrastructure
- Day 5: Auditing Web Applications
  - Web application security
  - Auditing the OWASP Proactive Controls

Course Information

Registration: Participants may enroll at our registration page

Course Cost: $2,400
10% discount before June 9, 2025 with Coupon Code: ***EarlyBird10***

Program Level: Intermediate

Delivery Method: Zoom webcast

Recommended CPE: 40 hours

Technical Requirements

Course delivery relies on a number of technologies. To ensure a good online class experience, students must have:

☑ A PDF reader for course books

☑ A reliable internet connection and web browser

☑ Zoom videoconferencing either with the application or in a browser

☑ Slack communication platform, using either an installed app or the web client

☑ A remote desktop protocol (RDP) client to access the lab environment

Detailed Outline

Day 1: Audit in the Enterprise and Cloud

This day provides the "on-ramp" for the highly technical audit tools and techniques used later in the course. After laying the foundation for the role and function of an auditor in the information security field, this day's material provides practical, repeatable and useful risk assessment methods that are particularly effective for measuring the security of enterprise systems, identifying control gaps and risks, and enabling us to recommend additional controls to address the risk. We finish off the day with an introduction to the risks and audit techniques that are important in cloud environments.

Day 1 Topics

- The auditor's role in the enterprise
- Basic auditing and assessment strategies
- Risk assessment
- The audit process
- Local network inventory monitoring
- Gaining visibility in the cloud
- Vulnerability scanning

Day 1 Lab Exercises

- Lab 1.1: Tool Setup
- Lab 1.2: Discovery
- Lab 1.3: Cloud Service Provider Tools
- Lab 1.4: Cloud Service Provider Inventory
- Capstone: CTF team setup and general information questions

Day 2: PowerShell, Windows System, and Domain Auditing

The majority of systems encountered on most enterprise audits are running Microsoft Windows in some version or another. The centralized management available to administrators has made Windows a popular enterprise operating system. The sheer volume of settings and configurable controls, coupled with the large number of systems often in use, makes auditing Windows servers and workstations a huge undertaking. In Day 2, we teach students how to audit Windows systems and Active Directory domains at scale. We begin with an introduction to Windows PowerShell, covering how to use the shell and moving on to writing and editing scripts which allow the auditor to perform repetitive tasks quickly and reliably.

Day 2 Topics

- PowerShell essentials
- Windows management instrumentation (WMI)
- Windows system measurements
- Users and groups
- Rights and permissions
- Auditing at scale

Day 2 Lab Exercises

- Lab 2.1: Intro to PowerShell
- Lab 2.2: Windows System Measurements
- Lab 2.3: Users, Permissions, and Logging
- Lab 2.4: Compliance and Testing at Scale
- Capstone: More tests against the Windows domain and lab Windows Server VM

Day 3: Auditing Linux

While many enterprises today use Microsoft Windows for their endpoint systems, Linux and other Unix variants are well-established as servers, security appliances and in many other roles. Given the nature of the work these Unix variants do, it is critical to ensure their security. Add to that the fact that mass centralized administration is less likely to occur with these systems, and auditing at scale becomes even more important. Day 3 uses Ubuntu (Debian-based) and Alma (Redhat-based) Linux as the example operating systems. We assume that students may have little or no Linux experience and build skill during the day accordingly.

Day 3 Topics

- Accreditation and snowflake servers
- Intro to Linux audit
- Bash scripting
- System hardening
- Services, network configuration and logging
- User and privilege management
- Full system audits and auditing at scale

Day 3 Lab Exercises

- Lab 3.1: Linux System Information and Permissions
- Lab 3.2: File Integrity, Kernel Settings, and Services
- Lab 3.3: Linux Logging
- Lab 3.4: Linux System Audits
- Capstone: Extra manual and OSQuery-based tests against the Linux hosts

Day 4: Auditing Cloud Infrastructure

Day 4 focuses on securing the enterprise network. The days are gone when a good firewall at the edge of the network is all we really need. In fact, in many enterprises, the network has no real "edge". Auditors should encourage their organizations to focus on security within the network with the same diligence as they use at the perimeter.

We begin with a discussion of private cloud technologies used in the modern enterprise. First, we look at the security issues related to virtualization hosts and present a list of controls which auditors should examine for the most commonly used hypervisors, with an emphasis on VMware products.

The next part of the day is dedicated to understanding containers and container orchestration tools and how they should be deployed and configured. Using the Center for Internet Security's (CIS) Benchmarks as guides, we take a look at how our container deployments should be secured and the important items to audit in those deployments. We wrap up this day with a discussion of serverless functions and their use in the enterprise.

Then, we examine how enterprises integrate cloud technologies into their portfolios and look at how cloud providers and their customers should share security responsibilities. We examine guidance from the Cloud Security Alliance and major cloud vendors to develop a list of items to review when auditing an organization's use of cloud services. We cover audit and security concerns with identity and access management, logging and monitoring, networking, infrastructure, compute resources, infrastructure as code, storage and databases. We examine the CIS benchmarks for the three largest cloud providers and review data gathering techniques to audit all three.

Day 4 Topics

- Private clouds and hypervisor security
- Application virtualization and container security
- Public cloud audit toolkit
- Auditing the public cloud:
  Shared responsibility; Identity and access management; Logging and monitoring; Networking and infrastructure; Compute resources; Infrastructure as code; Storage and databases
- Benchmarks and beyond

Day 4 Lab Exercises

- Lab 4.1: Docker and Kubernetes
- Lab 4.2: Cloud Identity and Access Management
- Lab 4.3: Cloud Infrastructure
- Lab 4.4: Cloud Benchmarks
- Capstone: New queries against the lab AWS range and local Kubernetes cluster

Day 5: Auditing Web Applications

Web applications seem to stay at the top of the list of security challenges faced by enterprises today. The organization needs an engaging and cutting-edge web presence, but the very technologies which allow the creation of compelling and data-rich websites also make it very challenging to provide proper security for the enterprise and its customers. Unlike other enterprise systems, our web applications are freely shared with the world and exposed to the potential for constant attack.

We begin this day with a discussion of the suite of technologies which make modern web applications work and the tools which auditors can use to identify, analyze, and manipulate these technologies as part of a well-designed and thorough security audit. We cover the technologies which make the web work: including HTML, HTTP, AJAX, web servers and databases. We also introduce the use of proxies in testing web applications by capturing, examining, and sometimes manipulating the traffic between a web client and the server.

We move on to introduce students to many of the resources available from the Open Web Application Security Project (OWASP), focusing on their Top 10 vulnerabilities list and the Top 10 Proactive Controls for web applications. From this foundation, we build a list of five critically important web development and deployment practices which serve as the basis for performing rigorous testing of web applications in the enterprise.

We dedicate most of the day to teaching the controls which can be used to secure applications and the skills needed to test and validate these controls. We develop and use a checklist for testing the most common and important security vulnerabilities. Throughout the day, students have the opportunity to use these tools to test sample web applications similar to those commonly deployed in today's enterprises. We also offer advice on how engineers, administrators, and developers can better secure the web technologies they design, implement and maintain. And finally, we discuss the best ways to report on findings and make useful recommendations.

Day 5 Topics

- Understanding web applications
- Server configuration
- Secure development practices
- Authentication
- Session tracking
- Data handling
- Logging and monitoring

Day 5 Lab Exercises

- Lab 5.1: Web App Auditing with Burp
- Lab 5.2: Server Configuration and Static Analysis
- Lab 5.3: Fuzzing with Burp
- Lab 5.4: Injection Flaws
- Capstone: Multiple tests against a traditional web app