# AUD507: Auditing Systems, Applications, and the Cloud

GSNA
Systems and Network Auditor
giac.org/gsna

6 Day Program | 36 CPEs | Laptop Required

## You Will Be Able To

- Apply risk-based decision making to the task of auditing enterprise security
- Understand the different types of controls (e.g., technical vs. non-technical) essential to performing a successful audit
- Conduct a proper risk assessment of an enterprise to identify vulnerabilities and develop audit priorities
- Establish a well-secured baseline for computers and networks as a standard to conduct audit against
- Perform a network and perimeter audit using a repeatable process
- Audit virtualization hosts and container environments to ensure properly deployment and configuration
- Utilize vulnerability assessment tools effectively to provide management with the continuous remediation information necessary to make informed decisions about risk and resources
- Audit a web application's configuration, authentication, and session management to identify vulnerabilities attackers can exploit
- Utilize automated tools to audit Windows and Linux systems
- Audit Active Directory Domains

**"Today's NetWars was definitely a challenge and for me I needed the team so we could all use our strengths. Excellent coverage of everything we've learned without repeating exact exercises we had done in the week. Good way to know I did understand what we've been learning all week. The workbook was a good reference to return to."**

—Carmen P., **U.S. Government**

***Controls That Matter – Controls That Work***

This course is organized specifically to provide a risk-driven method for tackling the enormous task of designing an enterprise security validation program, covering systems, applications, and the cloud. After covering a variety of high-level audit issues and general audit best practices, students will have the opportunity to delve into the technical "how-to" for determining the key controls that can be used to provide a high level of assurance to an organization. Real-world examples provide students with tips on how to verify these controls in a repeatable way, as well as many techniques for continuous monitoring and automatic compliance validation. These same real-world examples help the students learn how to be most effective in communicating risk to management and operations staff.

Students will leave the course with the know-how to perform effective tests of enterprise security in a variety of areas including systems, applications, and the cloud. The combination of high-quality course content, provided audit checklists, in-depth discussion of common audit challenges and solutions, and ample opportunities to hone their skills in the lab provides a unique setting for students to learn how to be an effective enterprise auditor.

## Business Takeaways

- Gain confidence in whether you have the correct security controls and they are working well
- Lower your audit costs with effective, efficient security audits
- Improve relevance of IT audit reporting, allowing the organization to focus on what really matters
- Improve security compliance while reducing compliance and security risks, protecting your reputation and bottom line

## Hands-On Training

This course goes beyond simply discussing the tools students could use; we give them the experience to use the tools and techniques effectively to measure and report on the risk in their organizations. AUD507 uses hands-on labs to reinforce the material discussed in class and develop the "muscle memory" needed to perform the required technical tasks during audits. In sections 1-5, students will spend about 25% of their time in lab exercises. The final section of the course is a full-day lab that lets students challenge themselves by solving realistic audit problems using and refining what they have learned in class.

Students learn how to use technical tests to develop the evidence needed to support their findings and recommendations. Each section affords students opportunities to use the tools and techniques discussed in class, with labs designed to simulate real-world enterprise auditing challenges and to allow the students to use appropriate tools and techniques to solve these problems.

**"The hands-on labs reinforce the learning from the book. I learn best when I can touch and feel the material being taught."**

—Rodney Newton, **SAP**

# Section Descriptions

### SECTION 1: Audit in the Enterprise and Cloud

This section 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 section'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 section with an introduction to the risks and audit techniques that are important in cloud environments.

**TOPICS:** Auditor's Role as it Relates to Policy Creation, Policy Conformance, and Incident Handling; Basic Auditing and Assessing Strategies; Risk Assessment; The Audit Process; Local Network Population Monitoring; Gaining Visibility in the Cloud; Vulnerability Scanning

### SECTION 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 this section, 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.

**TOPICS:** Windows Support and End of Life; PowerShell Command Essentials; PowerShell Scripting; Windows Management Instrumentation (WMI); Windows System Measurements; Users and Groups; Rights and Permissions; Group Policy and Logging; Auditing at Scale

### SECTION 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. This section 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. We begin with a discussion of system accreditation in a field where many servers are "snowflakes" – uniquely designed and different from our other enterprise systems. Then, we move on to discuss the fundamentals of Linux/Unix operating systems and the tools available to auditors for system testing and for developing audit scripts.

**TOPICS:** Accreditation and Snowflakes; Linux Audit Introduction; Bash Scripting; System Hardening; Services, Network Configuration and Logging; User and Privilege Management; Full System Audits

### SECTION 4: Auditing Cloud Infrastructure

This section 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.

**TOPICS:** Private Clouds and Hypervisor Security; Public Cloud Audit Toolkit; Auditing the Public Cloud: Part 1; Auditing the Public Cloud: Part 2; Auditing the Public Cloud: Part 3

### SECTION 5: Web Application Auditing

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.

**TOPICS:** Understanding Web Applications; Server Configuration; Secure Development Practices; Authentication; Session Tracking; Data Handling; Logging and Monitoring

### SECTION 6: Audit Wars

Audit Wars is a capstone exercise which allows students to test and refine the skills learned throughout the course. Using an online "capture the flag" (CTF) engine, students are challenged to audit a simulated enterprise environment by answering a series of questions about the enterprise network, working through various technologies explored during the course. At the conclusion of this section, students are asked to identify the most serious findings within the enterprise environment and to suggest possible root causes and potential mitigations.

**TOPICS:** Technologies included in the capstone exercise include: Cloud Services; Kubernetes; Windows Active Directory; Windows Workstations; Web Applications; OSQuery; Fleet DM; Linux

### Who Should Attend

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Security Compliance professionals
- Managers responsible for overseeing the work of an audit or security team
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to understand better what an auditor is trying to achieve, how they think and how to better prepare for an audit
- System and network administrators seeking to create strong change control management and detection systems for the enterprise
- Anyone looking to implement effective continuous monitoring processes within the enterprise


**GSNA**
**Systems and Network Auditor**
**giac.org/gsna**

### GIAC Systems and Network Auditor

The GIAC Systems and Network Auditor (GSNA) certification validates a practitioner's ability to apply basic risk analysis techniques and to conduct technical audits of essential information systems. GSNA certification holders have demonstrated knowledge of network, perimeter, and application auditing as well as risk assessment and reporting.

- Auditing, risk assessments, and reporting
- Network and perimeter auditing and monitoring, web application auditing
- Auditing and monitoring in windows and Unix environments