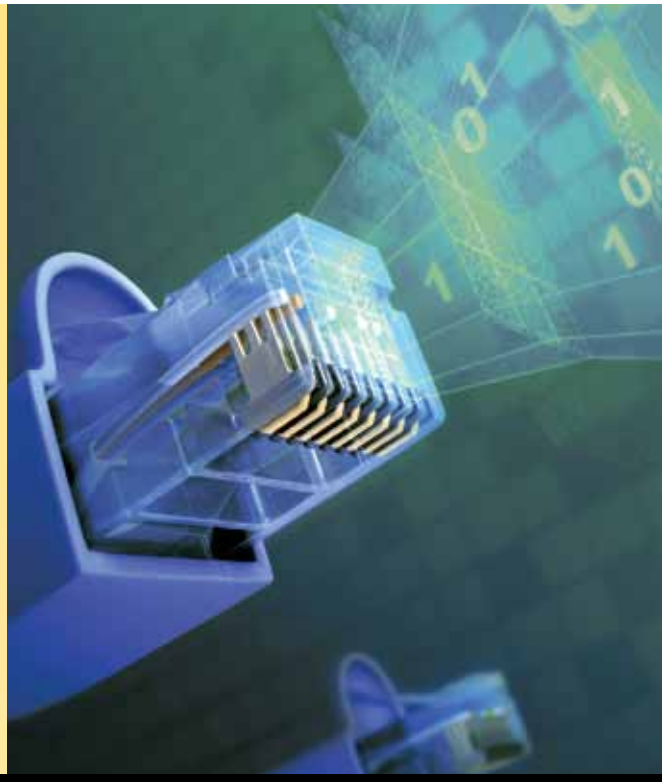
AUD507:
Auditing Networks, Perimeters, and Systems

Course Length: Six Days • 36 CPE Credits
Laptop Required

This course provides a risk-driven method for tackling the enormous task of designing an enterprise security validation program. After covering a variety of high-level audit issues and general audit best practice, you will have the opportunity to dive deep into the technical how-to for determining the key controls that can be used to provide a level of assurance to any organization. Tips on how to repeatedly verify these controls and techniques for automatic compliance validation will be given from real-world examples.



A great audit is more than marks on a checklist; it is the understanding of the what the underlying controls are, what the best practices are, and why.

While the primary audience for this course is auditors, system and security administrators will find very powerful techniques and processes for building continuous monitoring of systems and networks. Throughout the course, time is spent exploring how to determine what the correct "settings" are for an organization, how to abstract those settings into an automated process and how to ensure that the processes in the organization select and manage those settings correctly.

Every day of this course includes hands-on exercises. A variety of tools will be discussed and demonstrated during the lecture sections. These examples are then put into practice during labs so that you will leave knowing how to verify each and every control described in the class and know what to expect as audit evidence. Five of the hands-on days will give you the chance to perform a thorough technical audit of the technology being considered by applying the checklists provided in class to sample audit problems in a virtualized environment. Each student is invited to bring a Windows XP Professional or higher laptop for use during class. Macintosh computers running OS X may also be used with VMWare Fusion.

AUDIT CURRICULUM

SEC301
Intro to Information Security
GISF

↓

SEC401
SANS Security Essentials Bootcamp Style
GSEC

↓

AUD410
IT Security Audit and Control Essentials

↓

AUD423
SANS® +S™ Training for the CISA® Certification Exam

AUD429
IT Security Audit Essentials Bootcamp

↓

AUD507
Auditing Networks, Perimeters, and Systems
GSNA

AUD521
Meeting the Minimum: PCI/DSS 1.2: Becoming and Staying Compliant

↓

SEC440
20 Critical Security Controls: Planning, Implementing, and Auditing

SEC566
20 Critical Security Controls – In Depth

SANS www.sans.org

For more information, visit http://it-audit.sans.org

When registering, use this promo code ***AUD507***

What You Will Learn

- Audit planning and techniques
- Using Information Flow techniques to validate control placement
- Audit automation techniques
- Effective risk assessment for control specification
- Firewall and perimeter auditing
- A proven six-step audit process
- Time based auditing
- Effective network population auditing
- How to perform useful vulnerability assessments
- Uncovering back doors
- Building an audit toolkit
- Detailed router auditing
- Technical validation of network controls
- Web application auditing
- Audit tools

Who Should Attend:

- Auditors seeking to identify key controls in IT systems
- Audit professionals looking for technical details on auditing
- Managers responsible for overseeing the work of an audit or security team
- Administrators looking to create ongoing monitoring and alerting systems
- Security professionals newly tasked with audit responsibilities
- System and network administrators looking to better understand 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

Looking for a great IT audit resource?

SANS IT Audit Web site (**http://it-audit.sans.org**) is a community-focused site offering IT audit professionals a one-stop resource to learn, discuss, and share current developments in the field. It also provides information regarding SANS audit training, GIAC certification, and upcoming events. New content is added regularly, so please visit often. And don't forget to share this information with your fellow IT audit professionals.

GIAC Systems and Network Auditor (GSNA)

In the IT Audit world, the CISA and CIA credentials demonstrate that you have the minimum credentials necessary to act with competence as an IT auditor. The GSNA, however, is a sign that you have a significantly higher level of competence when it comes to the actual functioning, configuration and security of technical systems and networks. The GSNA tells clients and management that you not only know what the settings are, you know how to validate that those settings are working correctly. The GSNA also tells people that you know how to determine which controls are most important and how to determine if the controls that are in place are sufficient to meet the business and security needs of the organization.

Four Reasons to Get GIAC Certified:

- GIAC certification identifies those system and network administrators, security professionals, and software developers who know the tasks required to protect systems, networks, and code and who have the skills necessary to perform those tasks.
- 81% of hiring managers consider certifications a factor in their hiring decisions.
- 41% of InfoSec professionals say their organizations use certifications as a factor when determining salary increases.
- There is a strong demand for qualified information security professionals and GIAC certification proves you have the skills for the job.

Learn more about GIAC at www.giac.org.