
SANS
IT Audit
CURRICULUM
Audit Tips
and other
Free Audit Resources
Inside!
http://it-audit.sans.org

SANS IT Audit Curriculum Roadmap

SANS IT Audit curriculum features courses developed specifically for auditors and managers responsible for overseeing an IT audit or security team. Combining a mix of theory, hands-on and practical knowledge, SANS audit courses provide best practices and technical how-to's to help you conduct effective, thorough IT audits.

The courses are intensive, immersion training full of helpful techniques you can use immediately.

Core Courses

AUD407
Foundations of Auditing Information Systems

AUD507
Auditing Networks, Perimeters, and Systems
GSNA

SEC440
20 Critical Security Controls: Planning, Implementing and Auditing

SEC566
Implementing and Auditing the Twenty Critical Security Controls – In Depth

Specialized Courses

AUD305
Technical Communication & Presentation Skills

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

AUD429
IT Security Audit Essentials Bootcamp

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

Directors, Program Managers, Vice Presidents, CSO, CISO, CIO, CAO - While some of the courses will have periods of intense technical material (507, for instance), attendees at this level leave with key information to craft organizational direction and with a filter that allows you to know whether or not you're getting the whole story from both your internal staff and contractors.

Internal Auditors, External Auditors, Compliance Officers, ISOs, Program Managers, Communications Directors, MIS Managers & Directors, Managers of Technical Staff - Individuals working in these types of positions are in the "Sweet Spot" for the courses in SANS' Audit discipline. Not only will you walk away with lists of process improvements every day, but you will also have practical examples of workable implementations of those processes for your business.

System Administrators, Network Administrators, Incident Handlers, Penetration Testers, Technical Staff - You will leave SANS' Audit courses with a much firmer understanding of the relationship between your day to day practices and the mitigation of organizational risk. Not only will you learn how to approach technical problems from a process orientation, but you will leave with sets of tools that can dramatically reduce your day to day effort through ongoing compliance management and automation.

Dear Colleague,


David Hoelzer

Now more than ever, IT and IT Security Audit are coming to the forefront as critical business functions. Traditional financial audit remains a key regulatory and reporting requirement, but how can you assure the integrity of the information that serves as the basis for your financials without also assuring the security of the the systems that support that information? In many ways, this is the core of the Information Systems requirement under Sarbanes-Oxley.

The Information Security Audit strategies and techniques that have been incorporated into the various courses that SANS offers have been tailored to give you everything that you need to design, implement and manage an enterprise compliance program. Not only do we provide you the theoretical foundations and principles, but we also drill down into specific processes. Additionally, we seek to provide you with automated techniques that allow your Information Technology division to improve its effectiveness and provide a level of assurance above and beyond the typical internal SLA.

SANS courses are updated regularly to ensure the content is current and applies to the situations IT auditors face daily. Thousands of your fellow professionals have attended these courses and are using the information provided today. I'd like to invite you to come and attend one of these courses as soon as you can. You will leave every day of the class with a list of things that you will want to do as soon as you get back to your office!

Sincerely,

David Hoelzer

David Hoelzer
SANS Faculty Fellow
Curriculum Lead for SANS IT Audit Curriculum
Author of SANS Courses

CONTENTS

AUD407 Foundations of Auditing Information Systems 2-3
AUD507 Auditing Networks, Perimeters, and Systems 4-5
SEC440 20 Critical Security Controls: Planning, Implementing and Auditing . . . 6-7
SEC566 Implementing and Auditing the Twenty Critical Security Controls – In Depth 6-7
AUD429 IT Security Audit Essentials Bootcamp 8
AUD521 Meeting the Minimum: PCI/DSS 1.2: Becoming and Staying Compliant. . 9
AUD423 SANS® +S™ Training for the CISA® Certification Exam 10
Top Ten Audit Tips 11
Audit Resources 12
SANS Training Options 13

AUD407 Foundations of Auditing Information Systems

Six-Day Course
36 CPE Credits
Laptop Required

What You Will Learn

- Audit Frameworks
- The IS Audit Process
- Project Management for Auditors
- Data Collection Methodologies
- Regulations and Compliance
- Auditing, Vulnerability Testing & Penetration Testing
- Auditing Technical Controls
- Auditing Networks & Operating Systems
- Auditing Business Application Systems

Who Should Attend

- This class is designed for individuals who are tasked with auditing IT systems for implementation of organizational policies and procedures, risk, and policy conformance.
- Internal Auditors
- Assurance personnel
- Business and operational auditors
- System implementers/administrators
- Network security engineers
- DoD personnel/contractors

This course is a careful balance of audit process, governance, and compliance regulations as well as a hands-on introduction to the latest technology and tools.

This course is designed for business and operational auditors, security and assurance professionals, and system administrators, who want to develop the technical and operational knowledge to properly perform an IS audit. These auditing skills are in great demand as companies and agencies are required to comply with a growing number of regulations.

Students will learn the role of an auditor and the types of audits performed, various information security and audit frameworks, as well as the tools and techniques of auditing technical controls, foundations of auditing operating Systems, and foundations of auditing applications. Even seasoned audit and IT professionals will learn the value of performing IS audits as well as the business value of IS auditing.

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.

Delivery Methods
Live Events

407.1 *Hands On – Part 1:* Foundations of Auditing Information Systems

During the first day of the course students will begin to be exposed to the business of auditing information systems and their role in such an effort. Students will learn the business purpose and value of performing IS audits, as well as the role of an auditor and the types of audits that could be performed. In addition, students will have the opportunity to consider audit and information security frameworks which could serve as a foundation for audit programs or as a foundation for information assurance controls.

Topics: What is an IS Audit and Why Do One; The Roles of Auditors; Types of IS Audits; Audit Frameworks

407.2 *Hands On – Part 2:* Foundations of Auditing Information Systems

On the second day, students will continue their understanding of the foundational concepts of auditing information systems and begin to learn more about practical steps for performing and managing an audit. In addition, students will begin to examine the process of examining information assurance controls and the logistics necessary to effectively evaluate systems. Auditors will also be confronted with the importance of auditing systems in light of regulatory guidance and how compliance plays a part in the audit process.

Topics: The IS Audit Process; Project Management for Auditors; Data Collection Methodologies; Regulations & Compliance; Auditing; Vulnerability Testing; Penetration Testing

407.3 *Hands On:* Foundations of GRC Auditing

The third day of the course will introduce students to the importance of governance, risk, and compliance (GRC) concepts in the context of information system audits. This will lead students into an understanding of the relationship between business goals and IS controls used to manage risk. Formal risk management tools, frameworks, and techniques will be discussed and students will be exposed to available risk management programs during this day.

Topics: Introduction to Governance; Risk, & Compliance (GRC) Audits; Risk Assessment for Auditors; Connecting Business Objectives with Policy & Technology Controls; Formal Risk Assessment Models; Tools

407.4 *Hands On:* Foundations of Auditing Technical Controls

On day four, students will learn the importance of auditing technical controls as a part of an overall audit and assurance program. Students will be exposed to a model for evaluating technical controls and how they fit into the bigger picture of control audits. Students will have the opportunity to perform examples of technical control assessments and will have the chance to try their skills by learning practically how to audit network devices – including configuration files and network access control lists.

Topics: An Introduction to Auditing Technology Controls; Utilizing Scripts and Checklists in IS Audits; An Introduction to Auditing Network Devices; An Introduction to Auditing Network Perimeters

407.5 *Hands On:* Foundations of Auditing Operating Systems

During day five of the course, students will continue their exploration of technical assurance controls. Specifically, students will spend the day learning practical steps for auditing both Microsoft Windows and various flavors of Unix operating systems. Students will walk away from this day of the course with practical skills which will enable them to follow a repeatable process for auditing operating systems and the skills to identify risks in these systems. These skills will then be leveraged to consider how control audits of any system may be performed.

Topics: An Introduction to Auditing Operating Systems; Auditing User Accounts; Groups, & Permissions; Understanding Operating System Security Configurations; Vulnerability Management & Audit Scripts

407.6 *Hands On:* Foundations of Auditing Applications

The final day of this course will begin by examining the relationship between business goals and the application systems that are often used to enable those goals. Students will have the opportunity to learn practical skills for how to audit an application system from both a governance and technical control perspective. Students will be given hands on opportunities to perform an assessment on application systems in order to be prepared to perform these audits in the real world. In addition, students will be provided resources for further study in the audit field and next steps for furthering their careers in the profession.

Topics: An Introduction to Auditing Applications; Understanding an Application; Reviewing an Application's Development Cycle; Auditing an Application Step-by-Step; Course Conclusion; Next Steps; Available Audit Resources

AUD507 Auditing Networks, Perimeters, and Systems

Six-Day Program
36 CPE Credits
Laptop Required

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 IT auditing
- Managers responsible for overseeing the work of an IT audit or security team
- 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

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

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.

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.

GIAC Certification
www.giac.org

DoD 8570 Required
www.sans.org/8570

STI Masters Program
www.sans.edu

Delivery Methods
Live Events • Mentor • OnDemand • OnSite • vLive! • SelfStudy

Auditing Networks, Perimeters, and Systems is a hands-on course and is the most comprehensive, most technically advanced audit course on planet earth! Entry level IT auditors tend to earn $40,000 - $65,000 while more advanced auditors can earn up to $95,000. Those with the coveted GSNA certification often earn 8% more than those without.

507.1 Advanced Audit Foundations: Risk Assessment, Effective Reporting, and Modern Infrastructures

The first day of this course jumps right in with two advanced risk assessment processes that you can apply to your business immediately. Following this discussion, you will be able to analyze an existing set of controls, a business process, an audit exception, or a security incident, identify any missing or ineffective controls, and identify what corrective actions will eliminate the problem in the future. The afternoon will dig into how to audit the security of Virtualized and Cloud Computing environments.

Topics: Virtualization Security, Policy Conformance, and Incident Handling; Benefits of Various Auditing Standards and Certifications; Basic Auditing and Assessing Strategies, Risk Assessment; The Six-step Audit Process

507.2 *Hands On:* Auditing the Perimeter

Focus on some of the most sensitive and important parts of our information technology infrastructure: routers and firewalls. In order to properly audit a firewall or router, we need to clearly understand the total information flow that is expected for the device. Diagrams will allow the auditor to identify what objectives the routers and firewalls are seeking to meet, thus allowing controls to be implemented which can be audited. Overall, this course will teach the student everything needed to audit routers, switches, and firewalls in the real world.

Topics: Overview; Detailed Audit of a Router; Auditing Switches; Testing the Firewall; Testing the Firewall Rulebase; Testing Third-Party Software; Reviewing Logs and Alerts; The Tools Used

507.3 *Hands On:* Network Auditing Essentials

This day continues where day two left off, extending network and perimeter auditing to internal system validation and vulnerability testing, helping network security professionals to see how to use the tools and techniques described to audit, assess, and secure a network in record time. Following a defense-in-depth approach, learn how to audit perimeter devices, create maps of active hosts and services, and assess the vulnerability of those services. Hands-on exercises are conducted throughout the day so students have the opportunity to use the tools.

Topics: Introduction; War Dialing; Wireless; Mapping Your Network; Configuration Auditing of Key Services; Analyzing the Results; Follow-on Activities

507.4 *Hands On:* Web Application Auditing

We'll start with the underlying principles of Web technology and introduce a set of tools that can be used to validate the security of these applications. Then we will build and work through a checklist for validating the existence and proper implementation of controls to mitigate the primary threats found in Web applications.

Topics: Identify Controls Against Information Gathering Attacks; Process Controls to Prevent Hidden Information Disclosures; Control Validation of the User Sign-on Process; Examining Controls Against User Name Harvesting; Validating Protections Against Password Harvesting; Best Practices for OS and Web Server Configuration; How to Verify Session Tracking and Management Controls; Identification of Controls to Handle Unexpected User Input; Server-side Techniques for Protecting Your Customers and Their Sensitive Data

507.5 *Hands On:* Advanced Windows Auditing

Systems based on the Windows NT line (XP, 2003, Vista, 2008 and Windows 7) make up a large part of the typical IT infrastructure. Quite often, these systems are also the most difficult to effectively secure and control. This class gives you the keys, techniques, and tools to build an effective long term audit program for your Microsoft Windows environment.

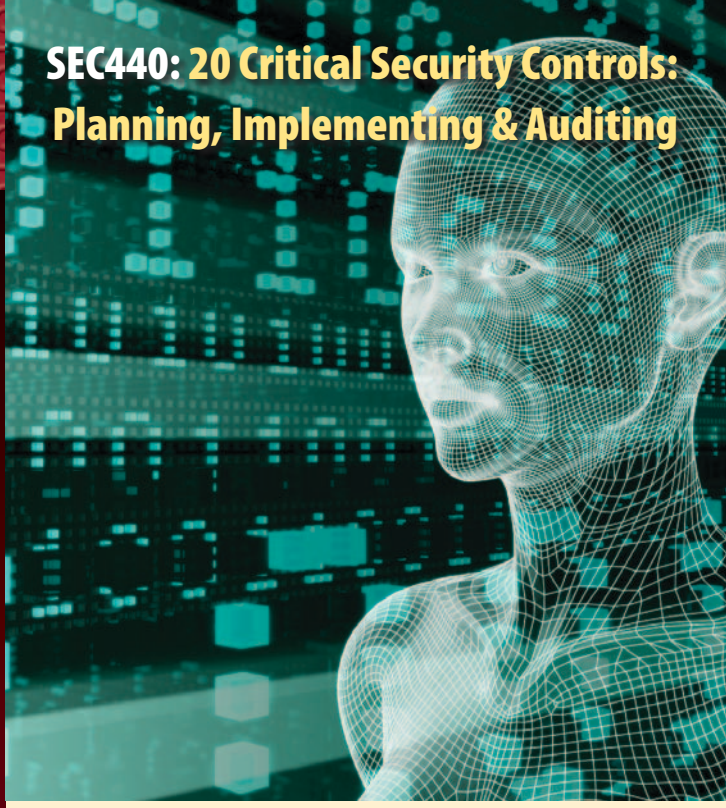
Topics: Progressive Construction of a Comprehensive Audit Program; Automating the Audit Process; Windows Security Tips and Tricks; Maintaining a Secure Enterprise

507.6 *Hands On:* Auditing Unix Systems

Students will gain a deeper understanding of the inner workings and fundamentals of the Unix operating system as applied to the major Unix environments in use in business today. Students will get to explore, assess, and audit Unix systems hands-on. Neither Unix nor scripting experience is required for this day.

Topics: Auditing to Create a Secure Configuration; Auditing to Maintain a Secure Configuration; Auditing to Determine What Went Wrong

SEC440/566



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

SEC440:
Two-Day Program
12 CPE Credits

SEC566:
Five-Day Course
30 CPE Credits
Laptop Required

Who Should Attend

- Information assurance auditors
- System implementers/administrators
- Network security engineers
- IT administrators
- DoD personnel/contractors
- Federal agencies/clients
- Private sector organizations looking for information assurance priorities for securing their systems
- Security vendors and consulting groups looking to stay current with frameworks for information assurance
- Alumni of SEC401, SEC501, SANS audit classes, MGT512, and for the SEC566 class specifically – alumni of SEC440 that want to get more hands-on training

Why this might be the most important course you'll take to boost your career in cyber security

What are the most important things we have to do to protect our systems? That is the question the defense industrial base CIOs asked the DoD when they learned their systems were leaking and losing some of America's most important military secrets to nation-state hackers. It is also the question that CIOs throughout government are asking when they learn from Government Accountability Office Congressional testimony that FISMA audits are not measuring security effectively. It is exactly the same question that is being asked in power companies and banks and oil and gas organizations and health care organizations. If you are the person who can not only answer the question, but also implement and/or audit the controls, you will be the game changer. It might not happen immediately, but it will happen.

These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them.

These courses (SEC440 & SEC566) will help you master specific, proven techniques and tools needed to implement and automate the 20 Critical Controls for Effective Cyber Security Defense, which are rapidly becoming accepted as the highest priority list of what must be completed and proven before anything else at nearly all serious and sensitive organizations.

These organizations defined the controls as their consensus for the best way to block the known attacks and the best way to help find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network through effective and widespread use of cost-effective automation.

For auditors, CIOs, and risk officers, this course is the best way to understand how you will measure whether the Top 20 controls are effectively implemented. It closely reflects the Top 20 Critical Security Controls found at **http://www.sans.org/critical-security-controls**.

SEC440: Delivery Methods
Live Events • OnSite

SEC566: Implementing and Auditing the 20 Critical Security Controls – In Depth

SEC440/566

Which Course Is Right For You?

SEC440: This course is an overview intended to help you obtain a high-level understanding of the controls and how they can be implemented. The focus is on strategic issues that an organization needs to know in order to effectively implement the controls.

SEC566: This is an in-depth, hands-on course with labs containing core implementation details to help an organization tactically implement the controls.

What is covered in each course:	SEC440	SEC566
Overview of the Controls	✔	✔
Executive Highlights	✔	
Detailed Coverage of the Controls		✔
Core Automation and Metrics	✔	✔
Strategic Coverage for Managers	✔	
Strategic Coverage for Auditors	✔	✔
Strategic Coverage for Implementers		✔
Core Checklists	✔	
Hands-on Labs		✔
Auditor Checklists	✔	✔
Strategic	✔	
Tactical		✔

Course Selection By Job Description

While someone could take both classes and obtain value from each, it is recommended that an organization send different staff to each class. The following is a chart showing which class would be more appropriate for different job descriptions:

	SEC440	SEC566
Executives	✔	
Technical Executives	✔	
Mid Level Managers	✔	✔
Auditors	✔	✔
Administrators		✔
Security Managers	✔	✔
Network Architects		✔
Security Engineers		✔
Line Managers	✔	
Staff	✔	

What You Will Learn

In both courses you'll learn important skills that you can take back to your workplace and use on your first day back on the job implementing and auditing each of the following controls:

15 critical security controls subject to automated collection, measurement, and validation:

- **Inventory of Authorized and Unauthorized Devices**
- **Inventory of Authorized and Unauthorized Software**
- **Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers**
- **Secure Configurations of Network Devices, Such as Firewalls, Routers, and Switches**
- **Boundary Defense**
- **Maintenance and Analysis of Security Audit Logs**
- **Application Software Security**
- **Controlled Use of Administrative Privileges**
- **Controlled Access Based On Need to Know**
- **Continuous Vulnerability Assessment and Remediation**
- **Account Monitoring and Control**
- **Malware Defenses**
- **Limitation and Control of Network Ports, Protocols, and Services**
- **Wireless Device Control**
- **Data Loss Prevention**

Additional critical controls (not directly supported by automated measurement and validation):

- **Secure Network Engineering**
- **Penetration Tests and Red Team Exercises**
- **Incident Response Capability**
- **Data Recovery Capability**
- **Security Skills Assessment and Training to Fill Gaps**

SEC566: Delivery Methods

Live Events • OnSite

AUD429 IT Security Audit Essentials Bootcamp

Two-Day Program
14 CPE Credits
Laptop Required

What You Will Learn

- A firm grasp of information security principles while also learning how to develop best practice audit checklists
- Key technologies, systems, and the tools that auditors use to examine complex systems such as large networks
- How to develop and evaluate audit controls that tie together electronic security of intellectual property with physical security to effectively measure overall security
- Initial concepts of auditing utilizing an enterprise risk management framework – building on security policy to evaluate controls used to protect information systems
- Hands-on auditing skills for both Microsoft Windows and Unix operating environments

Who Should Attend

Individuals entering the information security industry who are tasked with auditing organization policy, procedure, risk, or policy conformance

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.

This class was created to provide audit professionals and IT security personnel entering the IT Audit space with the key security principles and concepts and an understanding of how to apply them to information assurance and auditing.

In the information assurance and validation field, there is a real need for qualified auditors. Without professionals who can see how well we're performing security tasks, we create blind spots in our security vision, believing that we are perhaps more secure than we actually are. The trouble is finding a source of comprehensive Infosec information as it applies to auditing.

This course will help you get started in the field of information technology and security auditing by teaching you both audit theory and strong technical details. We cover the essentials of security, compliance, and IT auditing – everything you need, nothing you don't. As each topic is discussed, we will teach the underlying theories and then explain how and what about these topics require the attention of an auditor or compliance officer.

The course is taught in a hands-on environment so students receive the most benefit by actually trying what is described in the lectures. Throughout the class we will present all of the foundations of information security in connection with current information technology, while continually asking and answering "Why does an auditor care about this?"

Delivery Methods
OnDemand • OnSite • SelfStudy

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

AUD521

This intense two-day course gives you everything that you need to perform technical validations as a QSA, to oversee and implement a PCI compliant environment or to perform all of the testing necessary to complete an SAQ.

The PCI/DSS is a formalized set of best practices for security that must be followed by merchants and service providers who handle credit card data. How should a QSA (Qualified Security Assessor) evaluate an organization? How can your organization complete an SAQ (Self Assessment Questionnaire)? Regardless of the report generated by a QSA or an ASV (Authorized Scanning Vendor), how can you be sure that your organization is actually protected?

Not only will this course cover every requirement in the current PCI/DSS in detail, but you will leave the class with an easy to use toolkit that can be used to score the security of the technical controls that an organization has in place.

Whether you are responsible for PCI compliance, performing internal PCI assessments, implementing PCI or working as a QSA, this is a "Must Attend" course. An "unofficial" comment from a Visa employee responsible for overseeing PCI compliance was that, "Every QSA should be required to take this class. This is exactly what the standard is supposed to be."

Two-Day Course
12 CPE Credits
Laptop Required

What You Will Learn

- Requirements for compliance
- Compliance guidance for each control
- Suite of tools for validating technical compliance
- Explanation of alternative controls
- Discussion of determining scope for compliance requirements

Who Should Attend

- Managers overseeing PCI/DSS compliance
- Individuals completing the PCI SAQ (Self Assessment Questionnaire)
- Qualified Security Assessors (QSAs)
- External auditors performing PCI/DSS validations
- Security professionals operating in a PCI/DSS compliant environment
- Internal auditors desiring to validate interim compliance

Author Statement

This class is a lot of fun. In this short course we have the opportunity to examine a well written security standard and wrap an easy to use tool kit around it, allowing anyone who comes to perform fairly advanced technical validations through an exceedingly simple process. I think that any organization that has to adhere to PCI, any organization that performs external compliance validations and even the people who are maintaining the standard in the payment card industry will see immense value from attending.
- David Hoelzer

Delivery Methods

Live Events • OnDemand • OnSite • SelfStudy

AUD423

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

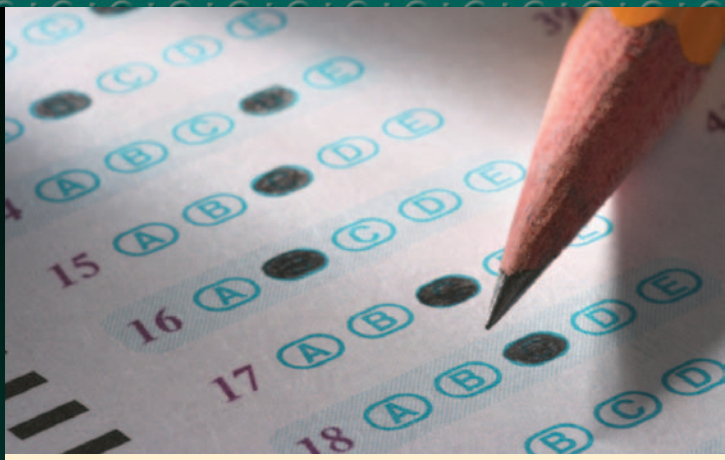
Six-Day Program
46 CPE Credits
Laptop Required

Who Should Attend

- Individuals that want to pass the CISA exam
- IT auditors
- System implementers/administrators
- Network security engineers
- Internal auditors
- Assurance personnel
- IT administrators
- DoD personnel/contractors

Author Statement

The CISA® exam is known internationally as a benchmark for information assurance auditors looking to validate their skills as an auditor. Since 1978 this certification program has existed to give organizations a standard by which to measure an auditor's understanding of core information security and auditing principles. Each year as ISACA updates their body of knowledge for the exam, the SANS Institute prepares an appropriate training course and program of study to give students the best possible chance to succeed in their efforts. In fact, in the past three years this course has been offered, the SANS Institute has seen a 100% pass rate on the exam for all of their students taking this course and following the program of study. This course has been written for the serious student that not only wants to pass the exam, but wants to definitively understand the course material and its practical application in a real-world setting.
- James Tarala



The SANS Certified Information Systems Auditor (CISA®) certification review course has been specifically written to help prepare for and to pass the CISA® exam while ensuring that the information presented is practical and applicable in daily life.

With over 40,000 certified CISAs worldwide, the CISA® certification has become a well-known standard for ensuring that auditors understand a common framework for performing information systems audits. Employers worldwide recognize the value of having certified employees and the level of validated experience that this certification can bring. And, especially with the regulations that organizations are facing, auditing and assurance is becoming an even more in-demand skill to possess.

The focus of this course is the six content areas (domains) that are outlined each year by ISACA, and students will have the opportunity to interact with a SANS instructor that is personally certified as a CISA®. While many training programs focus on simply presenting the information to students, SANS instructors are committed to not only presenting the information, but also to mentoring the students to ensure that they understand the information, can apply it to their professional careers, and can use that information to pass the CISA® exam.

Audit 423 includes hands-on bootcamp sessions, and students will receive practice tests.

Delivery Methods
OnSite

Top Ten Audit Tips

Auditing is never about trust or the lack thereof.
If you don't trust your employees, you're not auditing, you're investigating. If management doesn't trust the employees, then the employees should likely be replaced. Lacking trust, it will be difficult to lead the organization to success.

The primary role of an auditor is to measure and report on risk to the business and business objectives.
If an auditor loses sight of his actual role, it can lead to misleading findings. Management, and therefore auditors, must always keep their eyes on the prize.

A secondary objective is to reduce risk by raising the awareness of, at a minimum, management.
With awesome power comes awesome responsibility. Management asks us to tell them how the business is operating. If we fail to inform them in an effective way, then we fail in our responsibility to the business.

Never try to go toe-to-toe with a System Administrator on technical issues.
There's a reason they're the administrator and you're the auditor.

Auditing is never about catching people doing things wrong.
In fact, the best feeling as an auditor is to include commentary on some of the very right things that are going on in a business!

Communication is the most critical skill for an auditor; many times we are simply translating things that management has already heard into words that they understand.
In fact, as an auditor working with technical staff, you may forge relationships by choosing to adopt existing staff supported recommendations for your own audit report.

Always present recommendations in the framework of the currency of the organization.
If the business cares most about money, use dollars. Don't assume, however, that money is always the most motivating factor for management.

Trying to find everything is often a mistake.
Working with too large a scope can lead to a report that causes despair rather than increased security.

Never make promises.
Sometimes auditors discover truly gifted individuals who seem to be overlooked within the organization. While personal commendation is never bad, promising to tell management how wonderful the employee is can lead to dissatisfaction and turnover.

Never take it personally.
Despite every effort, auditors will sometimes face individuals who cannot separate business matters from personal matters. Worse, auditors will sometimes have to become the referee between business units or even individuals. Never let them see you sweat. Remember, it's only business.

Audit Resources

SANS IT Audit Blog

http://blogs.sans.org/it-audit

The SANS IT Audit Blog is the primary vehicle that SANS instructors use to provide information about current audit techniques, trends and tools. Readers are invited to write in questions and topic proposals that will be addressed in blog articles.

IT_Audit Twitter Feed

http://twitter.com/IT_Audit

Follow David Hoelzer's SANS Twitter Feed! Links to useful checklists, technical articles, upcoming events and even SANS discount codes are tweeted each day.

Free Audit & Testing Tools

http://it-audit.sans.org/community/downloads/

Looking for a tool? You may want to check here for useful free tools created by audit professionals.

SANS Audit Whitepapers

http://it-audit.sans.org/community/whitepapers.php

One of the most outstanding resources that SANS provides is the SANS Reading Room. At this link you can find a selection of the best whitepapers that cover topics of particular interest to IT Auditors.

SANS Training Options

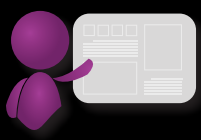
Contact SANS today to learn how we can build a custom training package using all of these formats for your organization. Having a variety of training formats allows SANS to develop the most technical and enriching training experience at the best price. We can tailor a program that allows you to take advantage of each delivery method and ensure your team receives not just the training, but the understanding they need to stay secure.

Number of People	Training Options
Individuals	Live Training Events, OnDemand, or vLive!
Groups of 15 or More	OnSite,OnDemand, or vLive!
Large Groups of 50 or More	**Enterprise Solutions:** OnDemand or vLive!

Live Training Events

The Most Trusted Name for Information Security Training

SANS offers classes throughout the year in many major US cities as well as Europe, Australia, Canada, Asia, India, and Dubai. These training events feature anywhere from one to over fifty classes at the same location. SANS events offer much more than just training – this is the place to network with other application security professionals, gain information on new vendor products, participate in onsite/online challenges and contests, and listen to world-class guest speakers.
www.sans.org/security-training/bylocation/index_na.php



SANS OnSite

Your Location - Your Schedule

With the SANS OnSite program you can bring a combination of high-quality content and world-recognized instructors to your location and realize significant savings in employee travel costs. www.sans.org/onsite

SANS vLive!

Live Virtual Instruction

SANS vLive! uses cutting-edge webcast technology to provide a live classroom experience with SANS top instructors, but delivers it over the web to students participating from their homes and offices. vLive! courses are interactive and allow students to share ideas, resources and experiences with their instructors before, during, and after training sessions. Each session is also recorded providing flexibility if a student needs to miss a session or simply wishes to review the material at a later date. www.sans.org/vlive

SANS OnDemand

Online Training and Assessment

SANS OnDemand allows students to access SANS' high-quality training 'anytime, anywhere' using SANS' advanced online delivery system. Students receive training from the same top-notch SANS instructors who teach at our live training events, and the system brings the true SANS experience right to your employees' desktops, which is convenient and saves you travel costs. Plus our integrated courseware, online assessments, hands-on exercises, and online mentor allow students to really grasp the material being taught! www.sans.org/ondemand