

IT Auditing: The First Step

Course Duration: 2 Day
CPE Hours: 16 Hours
Level: Beginner/Group-Live
Prerequisites: None
Advanced Preparation: None

This seminar has been completely rebuilt from the ground up to reflect the ever-shifting risks within the IT environment. In addition to physical and logical security risks, IT Auditors must contend with hackers, viruses, malware and spyware. Outsourcing and offshoring have dramatically changed the audit world. The Internet and wireless networks have magnified connectivity threats. Databases, data warehouses and storage management systems are now part of the basic audit requirements. The modules of this seminar have been structured such that the knowledge gained from completing one audit acts as a stepping stone to the next. This progression along with classroom discussion and comprehensive handouts will prepare participants for a transition into an IT audit role.

Who Should Attend:

This seminar is intended for new IT auditors, financial or operational auditors and new internal auditors.

Seminar Outline:

I) The IT Auditor: Identifying Risks and Protecting Information Assets

- Traditional IT risk environment
- Understanding new technology threats
- Performing an IT Risk Assessment
- Using tools to identify specific risks
- Building an IT Audit Plan

II) Auditing Data Centers

- Understanding physical security
- Perimeter protection techniques
- Access control mechanisms
- Defeating physical security
- Data storage and retrieval
 - ⇒ Protecting critical data
 - ⇒ Data warehousing and silos
- Logical security
 - ⇒ Identifying sensitive data
 - ⇒ Data classification
 - ⇒ Access restrictions
 - ⇒ User authentication techniques
 - ⇒ Defeating access controls
 - ⇒ Building better defenses
 - ⇒ Outsourcing and offshoring risks
- Backup and recovery
- Change management
- Documentation and prioritization of security risks

III) Disaster Preparedness and Business Continuation

- Identification and analysis of threats
 - ⇒ Natural disasters

- ⇒ Pandemic, loss of essential staff
- ⇒ Loss of connectivity
- ⇒ Attacks, viruses, spyware and other malware

- Disaster prevention and mitigation techniques
- Disaster recovery
- Offsite storage versus remote archiving
- Use of hot, cold and warm sites
- Business continuance
 - ⇒ Key person analysis
 - ⇒ Notification techniques
 - ⇒ Remote operational connectivity
 - ⇒ Enhanced security measures
- Testing, analysis and improving business continuance processes
- Documentation and analysis of identified risks

IV) Understanding and Auditing the Network

- Understanding network related risks
 - ⇒ The Internet
 - ⇒ The extranet
 - ⇒ The intranet
 - ⇒ ISPs
 - ⇒ Trading partner connectivity
 - ⇒ Web applications
 - ⇒ Wireless issues
 - ⇒ Unauthorized connectivity
- Network devices and components
- Mapping the network
- Network segmentation

- Risk identification and categorization
- Intrusion prevention and detection
- Incident response procedures
- Documentation and explanation of security issues

V) Database Identification and Security

- Fundamentals of database security
- Identifying databases throughout the organization
 - ⇒ Oracle
 - ⇒ MS SQL
 - ⇒ MySQL
 - ⇒ Sybase
- Undocumented and unauthorized instances
- Safe and sane testing techniques
- Documentation and presentation of identified risks

VI) Creating a Risk-Based IT Audit Plan

- Using Security Baselines for risk identification
- Selecting high-impact audits
- Sequencing and prioritizing audits
- Presentation of the IT Audit Plan

VII) Conclusion and Wrap-Up