INFOSECTRAIN

Become an Expert in Cyber Security Analyst

COURSE HIGHLIGHTS

- 120 hrs of instructor-led training
- Exam voucher included for CEH & ISO
- Certificate of Completion
- Access to the recorded sessions
- Certified &amp; Experienced Instructors

LEARNING PATH

- **Course 1**

CEH

- **Course 2**

SOC Analyst Expert

- **Course 3**

ISO 27001 LA

- **Master's Certificate**

You will get certificate by InfosecTrain

InfosecTrain's Cyber Security Analyst Training Course equips you with the fundamental toadvanced expertise required by the industry. It is a combo course that begins with CEH,progresses to SOC Analyst training, and concludes with ISO 27001 Lead Auditor. This InfosecTrain course will educate you on the various facets of Ethical Hacking, SOCAnalyst, and ISO 27001 compliance.

WHY CYBER SECURITY ANALYST COMBO TRAINING WITH INFOSECTRAIN?

InfosecTrain is a proficient security training and consulting organization across the globe,specializing in various IT security courses and services. Our Cyber Security Analyst training aims to explain to you all about ethical hacking, SOC operations and ISO 27001 compliance. You can leverage the following benefits with
InfosecTrain:

- We can help you present your qualifications and work experience for the designated profile.
- We provide a flexible training schedule.
- We provide post-training assistance.
- We create groups for discussion.
- We also provide a certificate of participation to each candidate

TARGET AUDIENCE

1. Technical Support Engineers
2. System Administrators
3. Security Consultants and Engineers
4. Cyber Security Analysts
5. SOC Analysts (L1, L2 &amp; L3)
6. Internal Auditors
7. Auditors, Project Managers or Consultants wanting to perform and lead ISMScertification audits
8. CxO and Senior Managers responsible for the IT governance of an enterprise and the management of its risks
9. Members of an information security team
10. Expert advisors of information technology and information security
11. Ethical Hackers
12. Network Administrator

PRE-REQUISITES

- Basic understanding of network essentials and core concepts, including server and network components
- Certified ISO/IEC 27001 Foundation Certification or basic knowledge of ISO/IEC 27001 is recommended.

EXAM INFORMATION

Exam Name	CEH V12	ISO 27001 LA
Exam Pattern	Multiple Choice Questions	Essay type
Exam Duration	240 minutes	180 minutes
No. of Questions	125	80
Passing Score	60%-85%	70%
Languages	English, German and Japanese	English

COURSE OBJECTIVES

- Ethical hacking fundamentals, cyber kill chain concepts, an overview of information security, security measures, and numerous information security laws and regulations.
- Footprinting concepts, methodologies, tools and countermeasures.
- Enumeration techniques include NFS enumeration and related tools, DNS cache snooping, and DNSSEC Zone walking along with the countermeasures.
- Concepts of vulnerability assessment, its categories and strategies, and first-hand exposure to the technologies used in industry.
- Phases of system hacking, attacking techniques to obtain, escalate, and maintain access on the victim and covering tracks.
- Malware threats, analysis of various viruses, worms, and trojans like Emotet and battling them to prevent data.
- Packet sniffing concepts, techniques, and protection against the same.
- Social engineering concepts and related terminologies like identity theft, impersonation, insider threats, social engineering techniques, and countermeasures.
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, use cases, and attack and defense tools.
- Security solutions like firewall, IPS, honeypots, evasion, and protection.
- Operational Technology (OT) essentials, threats, attack methodologies, and attack prevention. The concept of OT is a new addition.
- Recognizing the vulnerabilities in IoT and ensuring the safety of IoT devices.
- Encryption algorithms, Public Key Infrastructure (PKI), cryptographic attacks, and cryptanalysis.

- Cloud computing, threats and security, essentials of container technology, and serverless computing.
- Understand the Security Operation Center (SOC) team operations and architecture
- Understand Blue Team operations architecture
- In-depth knowledge of digital forensics, threat intelligence, incident response,
  vulnerability management, and endpoint analysis, VAPT
- Understand essential SOC tools like Splunk and Security Onion
- Understand how to recognize threats, implement countermeasures, and essential concepts of threat hunting
- Understand the advanced concepts of SIEM technology like ELK Stack Primer and IBM QRadar
- ISO/IEC 27001 certification process
- Information Security Management System (ISMS)
- The ISO/IEC 27000 family of standards
- Advantages of ISO/IEC 27001
- Fundamental of information and assets
- Fundamental principles of information security confidentiality, integrity, and availability
- Preparation of an ISO/IEC 27001 certification audit
- ISMS documentation audit
- Big data, artificial intelligence, machine learning, and cloud computing
- Auditing outsourced operations
- Communication during the audit
- Audit procedures: observation, document review, interview, sampling techniques, technical verification, corroboration, and evaluation
- Audit test plans

- Formulation of audit findings
- Audit approach based on risk
- Drafting a nonconformity report
- Audit documentation
- Quality review
- Conducting a closing meeting and conclusion of an ISO/IEC 27001 audit
- Evaluation of corrective action plans
- Establishing contact with the auditee
- Internal audit management program

COURSE CONTENT

C|EH V12

MODULE 1: INTRODUCTION TO ETHICAL HACKING

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Key topics covered:

- Elements of Information Security
- Cyber Kill Chain Methodology
- MITRE ATT&CK Framework
- Hacker Classes
- Ethical Hacking
- Information Assurance (IA)
- Risk Management
- Incident Management
- PCI DSS
- HIPPA
- SOX
- GDPR

MODULE 2: FOOT PRINTING AND RECONNAISSANCE

Learn how to use the latest techniques and tools to perform foot printing and reconnaissance, a critical pre-attack phase of the ethical hacking process.

Hands-On Lab Exercises:

Over 30 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform foot printing on the target network using search engines, web services, and social networking sites
- Perform website, email, whois, DNS, and network foot printing on the target network

MODULE 3: SCANNING NETWORKS

Cover the fundamentals of key issues in the information security world, including the basics of ethical hacking, information security controls, relevant laws, and standard procedures.

Hands-On Lab Exercises: Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform host, port, service, and OS discovery on the target network
- Perform scanning on the target network beyond IDS and firewall

MODULE 4: ENUMERATION

Learn various enumeration techniques, such as Border Gateway Protocol (BGP) and Network File Sharing (NFS) exploits, plus associated countermeasures.

Hands-On Lab Exercises: Over 20 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform NetBIOS, SNMP, LDAP, NFS, DNS, SMTP, RPC, SMB, and FTP Enumeration

MODULE 5: VULNERABILITY ANALYSIS

Learn how to identify security loopholes in a target organization’s network, communication infrastructure, and end systems.
Hands-On Lab Exercises:
Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform vulnerability research using vulnerability scoring systems and databases
- Perform vulnerability assessment using various vulnerability assessment tools

MODULE 6: SYSTEM HACKING

Learn about the various system hacking methodologies—including steganography, steganalysis attacks, and covering tracks—used to discover system and network vulnerabilities.
Hands-On Lab Exercises:
Over 25 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform buffer overflow attack to gain access to a remote system
- Escalate privileges using privilege escalation tools
- Escalate privileges in linux machine
- Hide data using steganography
- Clear Windows and Linux machine logs using various utilities
- Hiding artifacts in Windows and Linux machines

MODULE 7: MALWARE THREATS

Get an introduction to the different types of malware, such as Trojans, viruses, and worms, as well as system auditing for malware attacks, malware analysis, and countermeasures.

Hands-On Lab Exercises: Over 20 hands-on exercises with real-life simulated targets to build skills on how to:

- Gain control over a victim machine using Trojan
- Infect the target system using a virus
- Perform static and dynamic malware analysis

KEY TOPICS COVERED:

- Malware, Components of Malware
- APT
- Trojan
- Types of Trojans
- Exploit Kits
- Virus
- Virus Lifecycle
- Types of Viruses
- Ransomware
- Computer Worms
- Fileless Malware
- Malware Analysis
- Static Malware Analysis
- Dynamic Malware Analysis
- Virus Detection Methods
- Trojan Analysis
- Virus Analysis
- Fileless Malware Analysis
- Anti-Trojan Software
- Antivirus Software
- Fileless Malware Detection Tools

MODULE 8: SNIFFING

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks.
Hands-On Lab Exercises: Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform MAC flooding, ARP poisoning, MITM and DHCP starvation attack
- Spoof a MAC address of Linux machine
- Perform network sniffing using various sniffing tools
- Detect ARP poisoning in a switch-based network

KEY TOPICS COVERED:

- Network Sniffing
- Wiretapping
- MAC Flooding
- DHCP Starvation Attack
- ARP Spoofing Attack
- ARP Poisoning
- ARP Poisoning Tools
- MAC Spoofing
- STP Attack
- DNS Poisoning
- DNS Poisoning Tools
- Sniffing Tools
- Sniffer Detection Techniques
- Promiscuous Detection Tools

MODULE 9: SOCIAL ENGINEERING

Learn social engineering concepts and techniques, including how to identify theft attempts, audit human-level vulnerabilities, and suggest social engineering countermeasures.
Hands-On Lab Exercises: Over 4 hands-on exercises
with real-life simulated targets to build skills on how to:

> Perform social engineering using Various Techniques
> Spoof a MAC address of a Linux machine
> Detect a phishing attack
> Audit an organization’s security for phishing attacks

KEY TOPICS COVERED:

> Social Engineering
> Types of Social Engineering
> Phishing
> Phishing Tools
> Insider Threats/Insider Attacks
> Identity Theft

MODULE 10: DENIAL-OF-SERVICE

Learn about different Denial-of-Service (DoS) and Distributed DoS (DDoS) attack techniques, as well as the tools used to audit a target and devise DoS and DDoS countermeasures and protections. Hands-On Lab Exercises:
Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

> Perform a DoS and DDoS attack on a target host
> Detect and protect against DoS and DDoS attacks

KEY TOPICS COVERED:

- DoS Attack, DDoS Attack
- Botnets
- DoS/DDoS Attack Techniques
- DoS/DDoS Attack Tools
- DoS/DDoS Attack Detection Techniques
- DoS/DDoS Protection Tools

MODULE 11: SESSION HIJACKING

Understand the various session hijacking techniques used to discover network-level session management, authentication, authorization, and cryptographic weaknesses and associated countermeasures. Hands-On Lab Exercises: Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform session hijacking using various tools
- Detect session hijacking

KEY TOPICS COVERED:

- Session Hijacking
- Types of Session Hijacking
- Spoofing
- Application-Level Session Hijacking
- Man-in-the-Browser Attack
- Client-side Attacks
- Session Replay Attacks
- Session Fixation Attack
- CRIME Attack
- Network Level Session Hijacking
- TCP/IP Hijacking
- Session Hijacking Tools
- Session Hijacking Detection Methods
- Session Hijacking Prevention Tools

MODULE 12: EVADING IDS, FIREWALLS, AND HONEYPOTS

Get introduced to firewall, intrusion detection system, and honeypot evasion techniques; the tools used to audit a network perimeter for weaknesses; and countermeasures.

Hands-On Lab Exercises: Over 7 hands-on exercises with real-life simulated targets to build skills on how to:

- Bypass Windows Firewall
- Bypass firewall rules using tunneling
- Bypass antivirus

MODULE 13: HACKING WEB SERVERS

Learn about web server attacks, including a comprehensive attack methodology used to audit vulnerabilities in web server infrastructures and countermeasures.

Hands-On Lab Exercises: Over 8 hands-on exercises with real-life simulated targets to build skills on how to:

- Perform web server reconnaissance using various tools
- Enumerate web server information
- Crack FTP credentials using a dictionary attack

KEY TOPICS COVERED:

- Web Server Operations
- Web Server Attacks
- DNS Server Hijacking
- Website Defacement
- Web Cache Poisoning Attack
- Web Server Attack Methodology
- Web Server Attack Tools
- Web Server Security Tools
- Patch Management
- Patch Management Tools

MODULE 14: HACKING WEB APPLICATIONS

Learn about web application attacks, including a comprehensive web application hacking methodology used to audit vulnerabilities in web applications and countermeasures.

Hands-On Lab Exercises:

Over 15 hands-on exercises with real-life simulated targets to build skills on

- Perform web application reconnaissance using various tools
- Perform web spidering
- Perform web application vulnerability scanning
- Perform a brute-force attack
- Perform Cross-Site Request Forgery (CSRF) Attack
- Identify XSS vulnerabilities in web applications
- Detect web application vulnerabilities using various web application security tools

KEY TOPICS COVERED:

- Web Application Architecture
- Web Application Threats
- OWASP Top 10 Application Security Risks – 2021
- Web Application Hacking Methodology
- Web API
- Webhooks and Web Shell
- Web API Hacking Methodology
- Web Application Security

MODULE 15: SQL INJECTIONS

Learn about SQL injection attack techniques, injection detection tools, and countermeasures to detect and defend against SQL injection attempts.
Hands-On Lab Exercises: Over 4 hands-on exercises with real-life simulated targets to build skills on how to:

> Perform an SQL injection attack to extract database information
> Detect SQL injection vulnerabilities using various SQL injection detection tools

KEY TOPICS COVERED:

> SQL Injection
> Types of SQL injection
> Blind SQL Injection
> SQL Injection Methodology
> SQL Injection Tools
> Signature Evasion Techniques
> SQL Injection Detection Tools

MODULE 16: HACKING WIRELESS NETWORKS

Learn about wireless encryption, wireless hacking methodologies and tools, and Wi-Fi security tools
Hands-On Lab Exercises: Over 3 hands-on exercises
with real-life simulated targets to build skills on how to:
> Foot Print a wireless network
> Perform wireless traffic analysis
> Crack WEP, WPA, and WPA2 networks
> Create a rogue access point to capture data packets

KEY TOPICS COVERED:

> Wireless Terminology

> Wireless Networks

> Wireless Encryption

> Wireless Threats

> Wireless Hacking Methodology

> Wi-Fi Encryption Cracking

> WEP/WPA/WPA2 Cracking Tools

> Bluetooth Hacking

> Bluetooth Threats

> Wi-Fi Security Auditing Tools

> Bluetooth Security Tools

MODULE 17: HACKING MOBILE PLATFORMS

Learn about mobile platform attack vectors, Android vulnerability exploits, and mobile security guidelines and tools.

Hands-On Lab Exercises: Over 5

hands-on exercises with real-life simulated targets to build skills on how to:

> Hack an Android device by creating binary payloads

> Exploit the Android platform through ADB

> Hack an Android device by creating APK file

> Secure Android devices using various Android security tools

KEY TOPICS COVERED:

> Mobile Platform Attack Vectors

> OWASP Top 10 Mobile Risks

> App Sandboxing

> SMS Phishing Attack (SMiShing)

- Android Rooting
- Hacking Android Devices
- Android Security Tools
- Jailbreaking iOS
- Hacking iOS Devices
- iOS Device Security Tools
- Mobile Device Management (MDM)
- OWASP Top 10 Mobile Controls
- Mobile Security Tools

MODULE 18: IOT HACKING & OT HACKING

Learn about packet-sniffing techniques and how to use them to discover network vulnerabilities, as well as countermeasures to defend against sniffing attacks. Hands-On Lab Exercises: Over 2 hands-on exercises with real-life simulated targets to build skills on how to:

- Gather information using Online foot printing tools
- Capture and analyze IoT device traffic

KEY TOPICS COVERED:

- IoT Architecture
- IoT Communication Models
- OWASP Top 10 IoT Threats
- IoT Vulnerabilities
- IoT Hacking Methodology
- IoT Hacking Tools
- IoT Security Tools
- IT/OT Convergence (IIOT)

> ICS/SCADA
> OT Vulnerabilities
> OT Attacks
> OT Hacking Methodology
> OT Hacking Tools
> OT Security Tools

MODULE 19: CLOUD COMPUTING

Learn different cloud computing concepts, such as container technologies and server less computing, various cloud-based threats and attacks, and cloud security techniques and tools. Hands-On Lab Exercises: Over 5 hands-on exercises with real-life simulated targets to build skills on how to:

> Perform S3 Bucket enumeration using various S3 bucket enumeration tools
> Exploit open S3 buckets
> Escalate IAM user privileges by exploiting misconfigured user policy

KEY TOPICS COVERED:

> Cloud Computing
> Types of Cloud Computing Services
> Cloud Deployment Models
> Fog and Edge Computing
> Cloud Service Providers
> Container
> Docker
> Kubernetes
> Serverless Computing
> OWASP Top 10 Cloud Security Risks

> Container and Kubernetes Vulnerabilities
> Cloud Attacks
> Cloud Hacking
> Cloud Network Security
> Cloud Security Controls
> Cloud Security Tools

MODULE 20: CRYPTOGRAPHY

In the final module, learn about cryptography and ciphers, public-key infrastructure, cryptography attacks, and cryptanalysis tools. Hands-On Lab Exercises: Over 10 hands-on exercises with real-life simulated targets to build skills on how to:

> Calculate MD5 hashes
> Perform file and text message encryption
> Create and use self-signed certificates
> Perform email and disk encryption
> Perform cryptanalysis using various cryptanalysis tools

KEY TOPICS COVERED:

> Cryptography
> Encryption Algorithms
> MD5 and MD6 Hash Calculators
> Cryptography Tools
> Public Key Infrastructure (PKI)
> Email Encryption
> Disk Encryption
> Cryptanalysis
> Cryptography Attacks
> Key Stretching

SOC ANALYST

DOMAIN 1: BLUE TEAM OPERATIONS ARCHITECTURE

- Building a successful SOC
- Functions of SOC
- SOC Models & Types
- SOC Teams & Roles
- Heart of SOC- SIEM
- Gartner's magic quadrant – TOP SIEM
- SIEM guidelines and architecture

DOMAIN 2: SOC TOOLS

SPLUNK:

- Industrial requirements of Splunk in various fields
- Splunk terminologies, search processing language, and various industry use cases
- Splunk universal forwarder, data inputs, Correlating Events, Search fields

SECURITY ONION:

- Introduction to Security Onion : NSM
- Security Onion Architecture
- Walkthrough to Analyst Tools
- Alert Triage and Detection
- Hunt with Onion

> Web & Cloud Evidence

→ Cloud storage/backups, chat rooms, forums, social media posts, blog posts

> Evidence Forms

→ Laptops, desktops, phones, hard drives, tablets, digital cameras, smartwatches, GPS

> Chain of Custod

> What is the Chain of Custody?

> Why is it Important?

→ In regard to evidence integrity and examiner authenticity

> Guide for Following the Chain of Custody

→ Evidence collection, reporting/documentation, evidence hashing, write-blockers, working on a copy of original evidence

> Windows Investigations

> Artifacts

→ Registry, Event Logs, Prefetch, .LNK files, DLLs, services, drivers, common malicious locations, schedules tasks, start-up files

*nix Investigations

> Artifacts

> Equipment

→ Non-static bags, faraday cage, labels, clean hard drives, forensic workstations, Disk imagers, hardware write blockers, cabling, blank media, photographs, Laptops, desktops, phones, hard drives, tablets, websites, forum posts, blog posts, social media posts, chat rooms, Types of Hard Drive Copies visible data, bit for bit, slackspace

- Live Forensics
- Live Acquisition
    - → What is a live acquisition/live forensics? Why is it beneficial?
- Products
    - → SysInternals, Encase, memory analysis with agents, Custom Script
- Potential Consequences
    - → Damaging or modifying evidence making it invalid
- Post-Investigation
- Report Writing
- Evidence Retention
    - → Legal retention periods, internal retention periods
- Evidence Destruction
    - → Overwriting, degaussing, shredding, wiping
- Further Reading

TOOLS EXPOSURE PROVIDED IN THE ABOVE SECTION:

- Command-LINE for Windows / Linux
- Network Analysis: Wireshark, Network Miner
- Disk Based Forensics: FTK IMAGER, AUTOPSY, Encase
- Memory Forensics: MAGNATE & BELKASOFT RAM CAPTURE, DumpIt, Volatility, Volatility WorkBench
- Email Forensics: Manual & Automated Analysis

INCIDENT RESPONSE BASICS

- Introduction to Incident Response
- What is an Incident Response?
- Why is IR Needed?
- Security Events vs. Security Incidents
- Incident Response Lifecycle – NIST SP 800 61r2
- Incident Response Plan : Preparation, Detection & Analysis, Containment, Eradication, Recovery, Lessons Learned
- Case Study : Cyber Kill Chain in Incident Response
- Lockheed Martin Cyber Kill Chain
  - What is it, why is it used
- MITRE ATT&CK Framework
  - What is it, why is it used
- Preparation
- Incident Response Plans, Policies, and Procedures
- The Need for an IR Team
- Asset Inventory and Risk Assessment to Identify High-Value Assets
- DMZ and Honeypots
- Host Defences
  - HIDS, NIDS
  - Antivirus, EDR
  - Local Firewall
  - User Accounts
  - GPO

- Network Defences
  - → NIDS
  - → NIPS
  - → Proxy
  - → Firewalls
  - → NAC
- Email Defences
  - → Spam Filter
  - → Attachment Filter
  - → Attachment Sandboxing
  - → Email Tagging
- Physical Defences
  - → Deterrents
  - → Access Controls
  - → Monitoring Controls
- Human Defences
  - → Security Awareness Training
  - → Security Policies
  - → Incentives

DETECTION AND ANALYSIS

- Common Events and Incidents
- Establishing Baselines and Behavior Profiles
- Central Logging (SIEM Aggregation)
- Analysis (SIEM Correlation)

CONTAINMENT, ERADICATION, RECOVERY

- CSIRT and CERT Explained
  - → What are they, and why are they useful?
- Containment Measures
  - → Network Isolation, Single VLAN, Powering System(s) Down, Honeypot Lure
- Taking Forensic Images of Affected Hosts
  - → Linking Back to Digital Forensics Domain
- Identifying and Removing Malicious Artefacts
  - → Memory and disk analysis to identify artefacts and securely remove them
- Identifying Root Cause and Recovery Measures

LESSONS LEARNED

- What Went Well?
  - → Highlights from the Incident Response
- What Could be Improved?
  - → Issues from the Incident Response, and How These Can be Addressed
- Important of Documentation
  - → Creating Runbooks for Future Similar Incidents, Audit Trail
- Metrics and Reporting
  - → Presenting Data in Metric Form

- Further Reading

TOOLS EXPOSURE PROVIDED IN THE ABOVE SECTION:

- SYSINTERNAL SUITE
- Hash Calculator
- Online Sources
- CyberChef

DOMAIN 4: TI

- Introduction To Threat Intelligence
- Threat Actors
- Types of Threat Intelligence :
  - → Operational Intelligence
  - → Strategical Intelligence
  - → Tactical Intelligence

- CTI Skills: NIST NICE – CTI Analyst
- OODA Loop, Diamond Model of Intrusion Analysis
- Unleashing Threat Intel with Maltego, AlienVault OTX
- LOTL Based Techniques
- Malware Campaigns & APTs

ISO 27001:2022 LEAD AUDITOR

INTRODUCTION TO THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) AND ISO/IEC 27001

SECTION 1: TRAINING COURSE OBJECTIVES AND STRUCTURE

> General information
> Learning objectives
> Educational approach
> Examination and certification

SECTION 2: STANDARDS AND REGULATORY FRAMEWORKS

> What is ISO?
> The ISO/IEC 27000 family of standards
> Advantages of ISO/IEC 27001

SECTION 3: CERTIFICATION PROCESS

> Certification process
> Certification scheme
> Accreditation bodies
> Certification bodies

SECTION 4: FUNDAMENTAL CONCEPTS AND PRINCIPLES OF INFORMATION SECURITY

> Information and asset

> Information security

> Confidentiality, integrity, and availability

> Vulnerability, threat, and impact

> Information security risk

> Security controls and control objectives

> Classification of security controls

SECTION 5: INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

>Definition of a management system

> Definition of ISMS

> Process approach

> ISMS implementation

> Overview - Clauses 4 to 10

> Overview - Annex A

> Statement of Applicability

AUDIT PRINCIPLES, PREPARATION, AND INITIATION OF AN AUDIT

SECTION 6: FUNDAMENTAL AUDIT CONCEPTS AND PRINCIPLES

>Audit standards

> What is an audit?

> Types of audits

> Involved parties

> Audit objectives and criteria

SECTION 10: INITIATION OF THE AUDIT PROCESS

> The audit offer
> The audit team leader
> The audit team
> Audit feasibility
> Audit acceptance
> Establishing contact with the auditee
> The audit schedule

SECTION 11: STAGE 1 AUDIT

> Objectives of the stage 1 audit
> Pre on-site activities
> Preparing for on-site activities
> Conducting on-site activities
> Documenting the outputs of stage 1 audit

ON-SITE AUDIT ACTIVITIES

SECTION 12: PREPARING FOR STAGE 2 AUDIT

> Setting the audit objectives
> Planning the audit
> Assigning work to the audit team
> Preparing audit test plans
> Preparing documented information for the audit

SECTION 13: STAGE 2 AUDIT

- Conducting the opening meeting
- Collecting information
- Conducting audit tests
- Determining audit findings and nonconformity reports
- Performing a quality review

SECTION 14: COMMUNICATION DURING THE AUDIT

- Behavior during on-site visits
- Communication during the audit
- Audit team meetings
- Guides and observers
- Conflict management
- Cultural aspects
- Communication with the top management

SECTION 15: AUDIT PROCEDURES

- Overview of the audit process
- Evidence collection and analysis procedures
- Interview
- Documented information review
- Observation
- Analysis
- Sampling
- Technical verification

SECTION 16: CREATING AUDIT TEST PLANS

- Audit test plans
- Examples of audit test plans
- Guidance for auditing an ISMS
- Corroboration
- Evaluation
- Auditing virtual activities and locations

CLOSING OF THE AUDIT

SECTION 17: DRAFTING AUDIT FINDINGS AND NONCONFORMITY REPORTS

- Audit findings
- Types of possible audit findings
- Documenting the audit findings
- Drafting a nonconformity report
- The principle of the benefit of the doubt

SECTION 18: AUDIT DOCUMENTATION AND QUALITY REVIEW

- Work documents
- Quality review

SECTION 19: CLOSING OF THE AUDIT

> Determining audit conclusions
> Discussing audit conclusions
> Closing meeting
> Preparing audit report
> Distributing the audit report
> Making the certification decision
> Closing the audit

SECTION 20: EVALUATION OF ACTION PLANS BY THE AUDITOR

> Submission of action plans by the auditee
> Content of action plans
> Evaluation of action plans

SECTION 21: BEYOND THE INITIAL AUDIT

> Audit follow-up activities
> Surveillance activities
> Recertification audit
> Use of trademarks

SECTION 22: MANAGING AN INTERNAL AUDIT PROGRAM

> Managing an audit program
> Role of the internal audit function
> Main internal audit services and activities
> Audit program resources
> Audit program records
> Follow up on nonconformities
> Monitoring, evaluating, reviewing, and improving an audit program

INFOSECTRAIN

www.infosectrain.com | sales@infosectrain.com