



Training Synopsis

A brief overview





Information Security Management

- [Certified Information Systems Security Professional \(CISSP\)](#)
- [Certified Information Systems Manager \(CISM\)](#)
- [Information Security Management Systems \(ISO/IEC 27001\)](#)
- [Network Security Fundamentals \(Security+\)](#)
- [Ethical Hacking & Countermeasures \(CEH\)](#)
- [Computer Forensics \(CHFI\)](#)
- [Certified Security Analyst \(ECSA\)](#)
- [Application Security](#)
- [Malware Analysis](#)
- [Intrusion Analysis](#)
- [Wireless Security](#)
- [Cloud Security](#)



CISSP - Certified Information Systems Security Professional

CISSP is considered the Gold Standard for information security.

It consists of **10 domains** which include Cryptography, Access Controls, Operations Security, BCP & DR, Security Architecture & Models, Telecom & Internet Security, etc.

This certification is for information security professionals who wish to move up the ladder into security management. Needless to say, it is highly valued and respected with tremendous job opportunities in both India and abroad.

We conduct a workshop which covers the contents of the CBK (**Common Body of Knowledge**) from an exam perspective. Our workshops involve a high degree of peer level interaction and knowledge sharing.

Suggested study material would be

- All-in-one CISSP Exam Guide by **Shon Harris**
- CISSP Prep Guide Platinum Edition by **Ronald L Krutz**
- Official ISC² Guide to the CISSP CBK by **Harold Tipton**



CISSP...

Prerequisite

- 5 years of work experience with at least 2 years of specific domain expertise on any 2 domains of the ISC² CBK.
- Waiver of 1 year if you have 4 years of college education.
- Additional waiver if you have any one of the certifications outlined in the ISC² approved list.

Workshop Duration: 4 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 600
- 6 hours
- Pass mark 70% (Scaled score of 700 points out of a 1000 point score)
- 250 multiple choice questions
- Offline-paper exam-proctor required
- CISSP exam registration with ISC² www.isc2.org

Certification Process & Maintenance

- Endorsement from existing CISSP
- Minimum 20 contact hours of CPE (Continuing Professional Education)
- Minimum 120 contact hours of CPE during a fixed 3 year period
- US\$ 85 towards AMF (Annual Maintenance Fee)



CISM - Certified Information Systems Manager

CISM is suitable for those responsible for information security management in their organization.

Our workshop covers the **5 security management areas** of Information Security Governance, IS Risk Management, IS Program Development, IS Program Management, Incident Management & Response required for CISM.

Most information security professionals start their certification process with CISA become a CISSP and then move on to CISM. For professionals in the information security domain, a CISM would help differentiate their experience and qualification.

We conduct a workshop which covers the 5 security management areas as specified by ISACA (**Information Systems Audit and Control Association**) from an exam perspective and involves a high degree of peer level interaction and knowledge sharing.

Suggested study material would be

- CISM Review Manual from **ISACA**
- CISM Prep Guide by **Ronald L Krutz & Russel Dean Vines**



CISM...

Prerequisite

- 5 years of information security work experience with at least 3 years of specific domain expertise on any 3 or more of the job practice areas.
- Experience substitution of 2 years if you are already a CISA, CISSP or CBCP in good standing and 1 year if you have one of the skill based certifications specified by ISACA.

Workshop Duration: 3 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 615
- 4 hours
- Passing score of minimum 450 on a 200-800 point scale
- 200 multiple choice questions
- Offline-paper exam-proctor required
- CISM exam registration with ISACA www.isaca.org

Certification Process & Maintenance

- Minimum 20 contact hours of CPE (Continuing Professional Education)
- Minimum 120 contact hours of CPE during a fixed 3 year period
- US\$ 40 towards AMF (Annual Maintenance Fee)



ISO/IEC 27001

ISO/IEC 27001

ISO/IEC 27001 is the International Standards Organization (ISO) standard for Information Security Management Systems (ISMS). It consists of a set of best practices guideline which is implemented and audited prior to the organization getting certified.

Our workshop covers the clauses and controls of the international standard for ISMS along with the specific requirements of the Quality Management system. Participants learn how to implement and audit as per ISO 27001 guidelines and specifications supported by relevant checklists.

Prerequisite: Exposure to ISMS within any organization.

Workshop Duration: Foundation - 2 days
Implementation - 3 days
Internal Audit - 2 days
Lead Auditor - 5 days

Schedule: www.intellesecure.com/tc.php

Examination: Continuous assessment by accredited trainer followed by written examination

Relevant Certification: Foundation / Implementer / Internal Auditor / Lead Auditor for individual
ISO/IEC 27001 Certification for organization



Network Security Fundamentals

Network Security Fundamentals

This course teaches practical aspects of security and networking to give a better understanding of how to secure information, maintain privacy and avail the best of the computing resources available.

Our workshop is delivered by **senior security professionals** who manage network security on a regular basis. Participants learn from a practical perspective.

Prerequisite: Basic computing skills and some knowledge of networking concepts

Workshop Duration: 3 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 225
- 1.5 hours
- Pass mark 75%
- 100 multiple choice questions
- Online prime prometric exam
- **Security+** from CompTIA www.comptia.org OR
- **Security5** from EC-Council www.eccouncil.org OR
- **GSEC** - GIAC SANS Security Essentials from SANS Institute www.sans.org



Ethical Hacking & Countermeasures

CEH - Certified Ethical Hacker

This workshop helps you understand various tools which are used for hacking and how to develop countermeasures against these. Many of today's top hacking tools and methodologies like Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation will be taught in this course.

Our workshop is delivered by **senior security professionals** who handle vulnerability assessment & penetration testing (**VA / PT**) on a regular basis. Participants learn from a practical perspective.

Prerequisite: Adequate knowledge of networking and TCP/IP fundamentals

Workshop Duration: 5 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 500
- 4 hours
- Pass mark 70%
- 150 multiple choice questions
- NDA (Non Disclosure Agreement) to be signed
- **CEH** online prime prometric exam from EC-Council www.eccouncil.org





Computer Forensics

CHFI - Computer Hacking Forensic Investigator

This workshop helps you understand how to handle incident response and various ways and means to gather digital evidence to show proof of cyber crime in a court of law. Our workshop covers various tools of the forensic trade like Helix, Encase, etc. and shows you a step by step approach to handling an investigation.

Our workshops is delivered by **professional computer forensic investigators** who handle incident response and digital forensics on a regular basis.

Prerequisite: Adequate knowledge of networking and hacking methodologies

Workshop Duration: 5 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 250
- 2 hours
- Pass mark 70%
- 50 multiple choice questions
- NDA (Non Disclosure Agreement) to be signed
- **CHFI** online prime prometric exam from EC-Council www.eccouncil.org





Certified Security Analyst

ECSA - EC-Council Certified Security Analyst

This workshop complements CEH by exploring the analytical phase of ethical hacking. It gives an in-depth perspective of advanced hacking and penetration testing methodologies. Participants understand how to analyze the outcome of using security tools and security testing techniques.

Our workshops is delivered by **professional security analysts** who handle IT infrastructure security assessments on a regular basis.

Prerequisite: Adequate knowledge of hacking methodologies and must have completed CEH

Workshop Duration: 5 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 300
- 2 hours
- Pass mark 70%
- 50 multiple choice questions
- NDA (Non Disclosure Agreement) to be signed
- **ECSA** online prime prometric exam from EC-Council www.eccouncil.com





Application Security

Application Security

Application Security training helps you understand the vulnerabilities in web applications and how to prevent these by adopting secure design principles in all phases of the **SDLC** (**S**oftware **D**evelopment **L**ife **C**ycle). Our training covers security testing, code review, threat modeling using various tools and methodologies prescribed by **OWASP** (**O**pen **W**eb **A**pplication **S**ecurity **P**roject).

Participants will get a better understanding of vulnerabilities and the various techniques used to test applications and mitigate risk.

Prerequisite: Exposure to writing applications using ASP.NET or Java / J2EE and / or requirement to audit applications from a security perspective.

Workshop Duration: 2 days

Schedule: www.intellesecure.com/tc.php

Examination: Relevant certifications (Not available in India as of now)

ECSP - EC-Council Certified Secure Programmer from EC-Council www.eccouncil.org

OR

GWAPT - GIAC Web Application Penetration Tester from SANS Institute www.sans.org



Malware Analysis

Malware Analysis

Malware Analysis helps you understand how to reverse engineer malicious programs using a variety of system and network monitoring utilities, a disassembler, a debugger, and other tools covering dynamic and static analysis on portable executable programs.

Security Specialists must be able to perform rapid analysis on the malware and understand the functionality of the malware, without which, remediation efforts usually fail to meet expectations.

This course gives a better understanding of the steps and processes involved in malware analysis.

Prerequisite: Adequate knowledge of network security, computer forensics and incident response.

Workshop Duration: 2 days

Schedule: www.intellesecure.com/tc.php

Examination: Relevant certification (Not available in India as of now)

GREM - GIAC Reverse Engineering Malware from SANS Institute www.sans.org



Intrusion Analysis

Intrusion Analysis

Intrusion Analysis helps you understand how to examine the packet decode from network intrusion detection systems.

A skilled intrusion analyst will be able to analyze packets to reduce the likelihood of false positives and also be able to proactively update signatures and apply new filters to deal with emerging threats.

Participants will understand how to use Snort to detect intrusions, read, interpret and analyze network traffic and related log files. This course gives a better understanding of intrusion analysis from an industry perspective.

Prerequisite: Adequate knowledge of network security, intrusion detection, log analysis and incident response.

Workshop Duration: 2 days

Schedule: www.intellesecure.com/tc.php

Examination: Relevant certification (Not available in India as of now)

GCIA - GIAC Certified Intrusion Analyst from SANS Institute www.sans.org



Wireless Security

Wireless Security

Wireless Security training helps provide you with the necessary skills for implementing and managing wireless security in the enterprise. Wireless Networks are inherently more vulnerable than wired networks. Participants will get hands-on experience in configuring, testing, and implementing a broad variety of wireless security solutions.

Our training will help you understand how to use various tools such as NetStumbler, AiroPeek, Kismet, Wireshark and how hackers attack 802.11 based networks including WEP cracking.

Prerequisite: Exposure to wireless networking.

Workshop Duration: 2 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 225
- 1.5 hours
- Pass mark 70%
- 60 multiple choice questions
- **CWNP** online prime prometric exam www.cwnp.com (Planet 3 Wireless/CWNP)





Cloud Security

Cloud Security

Cloud Security is based on the best practice guidelines outlined by **Cloud Security Alliance (CSA)** and the recommendations given by the **European Network and Information Security Agency (ENISA)**, namely,

- *CSA's Security Guidance for Critical Areas in Cloud Computing*
- *ENISA Cloud Computing: Benefits, Risks and Recommendations for Information Security*

Prerequisite: Basic understanding of security fundamentals, firewalls, secure development, encryption and identity management

Workshop Duration: 2 days

Schedule: www.intellesecure.com/tc.php

Examination

- US\$ 295
- 1 hour
- Pass mark 80%
- 50 multiple choice questions
- **CCSK** online prometric exam <https://ccsk.cloudsecurityalliance.org/>

