

Course Title : CISSP

Course Introduction:

More and more today, companies rely on the network for the storage and fast retrieval of mission-critical corporate data and information. Securing these massive amounts of sensitive data is critical for the success of the organization and one of the main reasons that security has become one of the most important areas of IT specialization available. As the first ANSI ISO accredited credential in the field of information security, the Certified Information Systems Security Professional CISSP certification provides information security a globally recognized standard of achievement. Considered the gold standard in the information security realm, this credential gives prospective employers an invaluable tool in validating candidates' expertise in securing an enterprise, and provides global recognition for top information security professionals.

Course Objectives

Upon completion of the Certified Information Systems Security Professional (CISSP) course, the student will be able to:

- Implement solid security practices
- Perform in depth risk analysis
- Configure proper access rights and permissions
- Implement access control
- Secure data as it crosses the network
- Implement proper change control
- Understand methods used to attack resources
- Understand the systems development life cycle
- Perform security audits
- Develop a business continuity plan
- Understand laws on and about computer crime

Course Prerequisites

- The CISSP Certification program is targeted at professionals with at least 4 years of experience in the information security field or 3 years of experience and a college degree (or equivalent life experience). Please review the [CISSP Certification web site](#) for complete information about CISSP Certification rules and requirements

Target Group

This course is beneficial to any system or field engineers responsible for any aspect of network security . This course is a must for any students attempting the CISSP

certification, and is ideal for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.

Learning Level

Intermediate / Advanced

Course Duration

18 days (3 hours /day)

Benefits of a CISSP (both to the individual and to the Enterprise)

People are the key to a secure organization.

Technological solutions alone cannot protect an organization's critical information assets. Employers demanding qualified information security staff give their organizations a leading edge by providing the highest standard of security for their customers', employees', stakeholders' and organizational information assets. (ISC)², the only not-for-profit body charged with maintaining, administering and certifying information security professionals via the compendium of industry best practices, the (ISC)² CBK[®], is the premier resource for information security professionals worldwide.

Benefits of Certification to the Professional

- Demonstrates a working knowledge of information security
- Confirms commitment to profession
- Offers a career differentiator, with enhanced credibility and marketability
- Provides access to valuable resources, such as peer networking and idea exchange

Benefits of Certification to the Enterprise

- Establishes a standard of best practices
- Offers a solutions-orientation, not specialization, based on the broader understanding of the (ISC)² CBK
- Allows access to a network of global industry and subject matter/domain experts
- Makes broad-based security information resources readily available
- Adds to credibility with the rigor and regimen of the certification examinations
- Provides a business and technology orientation to risk management

Course Topics/Outlines

- Information Security & Risk Management
- Security Architecture and Design
- Access Control
- Application Security -
- Operations Security -
- Physical Security
- Cryptography
- Telecommunications & Network Security -
- Business Continuity & Disaster Recovery Planning -
- Legal, Regulations, Compliance & Investigations

CISSP Certification Requirements

Beginning **30 April 2008**, members with the affected certification(s) must earn the minimum number of CPEs annually during each year of the three-year certification cycle. Although members may earn more than the minimum CPEs required for credential maintenance for the three-year cycle, they are still required to earn and submit the minimum *annual* number to maintain their certification in **good standing**.

▪ **What are the new requirements for the CISSP?**

Currently, to maintain the CISSP certification, a member is required to earn and submit a total of 120 CPEs by the end of their three-year certification cycle and pay the AMF of US\$85 during each year of the three-year certification cycle before the annual anniversary date. **With the new changes effective 30 April 2008**, CISSPs are required to earn and post a minimum of 20 CPEs (of the 120 CPE certification cycle total requirement) and pay the AMF of US\$85 during each year of the three-year certification cycle before the member's certification or recertification annual anniversary date. For CISSPs who hold one or more concentrations, CPEs submitted for the CISSP concentration(s) will be counted toward the annual minimum CPEs required for the CISSP.

Effective **1 October 2007**, professional work experience requirements for the CISSP® will increase from four to five years, and direct full-time security professional work experience will be required in two or more of the ten CISSP® CBK® domains. A new

endorsement policy will also be in effect, requiring anyone who passes a CISSP, CAP®, or SSCP® exam to have their qualifications endorsed by another CISSP credential holder.

CISSP professional experience includes:

- Work requiring special education or intellectual attainment, usually including a liberal education or college degree.
- Work requiring habitual memory of a body of knowledge shared with others doing similar work.
- Management of projects and/or other employees.
- Supervision of the work of others while working with a minimum of supervision of one's self.
- Work requiring the exercise of judgment, management decision-making, and discretion.
- Work requiring the exercise of ethical judgment (as opposed to ethical behavior).
- Creative writing and oral communication.
- Teaching, instructing, training and the mentoring of others.
- Research and development.
- The specification and selection of controls and mechanisms (i.e. identification and authentication technology) (does not include the mere operation of these controls).
- Applicable titles such as officer, director, manager, leader, supervisor, analyst, designer, cryptologist, cryptographer, cryptanalyst, architect, engineer, instructor, professor, investigator, consultant, salesman, representative, etc. Title may include programmer. It may include administrator, except where it applies to one who simply operates controls under the authority and supervision of others. Titles with the words "coder" or "operator" are likely excluded.

Waiver of Experience:

If certain circumstances apply and with appropriate documentation, candidates are eligible to waive a maximum of two years of professional experience as follows:

- **One-year waiver of the professional experience requirement for education.**

Candidates can substitute a maximum of one year of direct full-time security professional work experience described above if they have a four-year college degree OR a Master's Degree in information security from a U.S. National Center of Academic Excellence in Information Security (CAEIAE) or regional equivalent.

If you hold both a four-year degree and a Master's degree, you may only apply for a one-year waiver of experience.

▪ **One-year waiver of the professional experience requirement for holding an additional credential:**

- CERT Certified Computer Security Incident Handler (CSIH)
- Certified Business Continuity Planner (CBCP)
- Certified Computer Crime Investigator (Advanced) (CCCI)
- Certified Computer Crime Prosecutor
- Certified Computer Examiner (CCE)
- Certified Fraud Examiner (CFE)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Internal Auditor (CIA)
- Certified Protection Professional (CPP)
- Certified Wireless Security Professional (CWSP)
- CompTIA Security+
- Computer Forensic Computer Examiner (CFCE)
- GIAC Security Essentials Certification (GSEC)
- GIAC Certified Firewall Analyst (GCFW)
- GIAC Certified Intrusion Analyst (GCIA)
- GIAC Certified Incident Handler (GCIH)
- GIAC Certified Windows Security Administrator (GCWN)
- GIAC Certified UNIX Security Administrator (GCUX)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Information Security Officer (GISO)
- GIAC IT Security Audit Essentials (GSAE)
- GIAC Security Expert (GSE)
- GIAC Certified ISO-17799 Specialist (G7799)
- GIAC Security Leadership Certification (GSLC)
- GIAC Systems and Network Auditor (GSNA)
- GIAC Certified Security Consultant (GCSC)
- Microsoft Certified Systems Administrator (MCSA)
- Microsoft Certified Systems Engineer (MCSE)
- Master Business Continuity Planner (MBCP)
- System Security Certified Practitioner (SSCP)

CISSP® - How to Certify - Exam Information

There are four processes a candidate must successfully complete to become a certified CISSP®:

- Examination
- Certification
- Endorsement
- Audit

Examination

To sit for the CISSP examination, a candidate must:

- Sign up for the examination date and location
- Submit the examination fee
- Assert that he or she possesses a minimum of five years of **professional experience** in the information security field or four years plus a college degree. Or, an Advanced Degree in Information Security from a National Center of Excellence or the regional equivalent can substitute for one year towards the five-year requirement.
- Complete the Examination Agreement, attesting to the truth of his or her assertions regarding professional experience, and legally committing to the adherence of the **(ISC)²Code of Ethics**
- Successfully answer four questions regarding criminal history and related background

Certification

To be issued a certificate, a candidate must:

- Pass the CISSP examination with a scaled score of 700 points or greater
- Submit a properly completed and executed **Endorsement Form**
- Successfully pass an audit of their assertions regarding professional experience, if the candidate is selected for audit

Endorsement

Once a candidate has been notified they have successfully passed the CISSP examination, he or she will be required to have his or her application endorsed before the credential can be awarded.

The endorser attests that the candidate's assertions regarding professional experience are true to the best of their knowledge, and that the candidate is in good standing within the information security industry.

More on endorsement.

Audit

Passing candidates will be randomly selected and audited by (ISC)² Services **prior to** issuance of any certificate. Multiple certifications may result in a candidate being audited more than once.

Maintenance Requirements

Recertification is also required every three years, with ongoing requirements to maintain

your credentials in good standing. This is primarily accomplished through continuing professional education [CPE], 120 credits of which are required every three years. A minimum of 20 CPEs must be posted during each year of the three-year certification cycle. More information on qualifying CPEs will be available upon certification.

CISSPs must also pay an annual maintenance fee of \$85 per year.