International Information Systems Security Certification Consortium (ISC)²

Website:	www.isc2.org
E-mail:	infoisc2@isc2.org
Address:	2494 Bayshore Boulevard, Suite 201 Dunedin, FL 34698, USA
Phone:	+1 703 891 0782
Fax:	+1 727 738 8522

The International Information Systems Security Certification Consortium or (ISC)² is a non-profit organisation incorporated in 1989 in the United States and governed by an elected Board of Directors. In addition to headquarters in the United States (ISC)² also has representative offices in London and Hong Kong. The Consortium's four main areas of activity are:

- Definition and maintenance of the information security common body of knowledge
- Certification of information security professionals and practitioners
- Administration of information security training and examinations
- Information security credentials maintenance

The International Information Systems Security Certification Consortium offers the following qualifications:

- Certified Information Systems Security Professional (CISSP)
- Systems Security Certified Practitioner (SSCP)
- (ISC)² Associate

Additionally, the following concentrations may be pursued by those who hold the CISSP designation:

- Information Systems Security Architecture Professional (ISSAP)
- Information Systems Security Management Professional (ISSMP)
- Information Systems Security Engineering Professional (ISSEP)

All of these qualifications and concentrations are introduced in this handbook. (ISC)² partner and supporting organisations include the Computer Security Institute, Canadian Information Processing Society, Data Processing Management Association, Idaho State University, Information Systems Security Association, MIS Training Institute, and the International Federation for Information Processing. For up to date information on (ISC)² and its activities please visit www.isc2.org.

Certified Information Systems Security Professional (CISSP)

The CISSP designation is one of the most respected and most comprehensive professional-level information security qualifications. Awarded to information security professionals for more than a decade CISSP has proven its professional standing and enjoys unrivalled recognition in the industry. Certified Information Systems Security Professionals have demonstrated mastery of the following domains of the information security common body of knowledge as defined by the International Information Systems Security Certification Consortium:

- Security Management Practices
- Security Architecture and Models
- Access Control Systems & Methodology
- Application Development Security
- Operations Security
- Physical Security
- Cryptography
- Telecommunications, Network, & Internet Security
- Business Continuity Planning
- Law, Investigations, & Ethics

CISSP candidates must meet the following requirements in addition to obtaining a passing score on the CISSP examination:

- Subscribe to the (ISC)^2 Code of Ethics
- Have minimum 4 years of direct full-time security professional work experience in one or more of the ten domains of the information systems security Common Body of Knowledge (CBK) or 3 years of direct full-time security professional work experience in one or more of the ten domains of the information systems security Common Body of Knowledge (CBK) with a college degree. Additionally, a Master's degree in information security from a U.S. National Centre of Excellence can substitute for one year towards the four-year requirement.

The CISSP examination, along with all other examinations conducted by (ISC)^2, is regularly held in countries where there is a substantial number of candidates – a full and up to date list is available online from (ISC)^2.

The examination is closed-book and consists of 250 multiple-choice questions of which 25 questions are questions in development; these are not scored. Candidates have 6 hours to attempt the exam and must obtain

a scaled score of 700 or more (out of 1,000) to pass. Scoring is done by an independent professional measurement organisation and not the (ISC)² themselves. Unlike most other examinations described in this handbook (ISC)² examinations are pen and paper examinations.

To aid CISSP candidates an official study guide is available online from the (ISC)²; official CISSP review seminars are regularly conducted by the (ISC)² Institute, the training arm of the Consortium. Additionally, a number of training organisations offer CISSP preparation courses. Conventional instructor-led and online tuition is available. For a current list of approved training offerings visit (ISC)² at www.isc2.org.

Maintaining the CISSP certification involves earning 120 hours of continuing professional education (CPE) credits every three years. CPE credits may be earned in different ways, including but not to limited to attending information security seminars, conferences, and courses; teaching information security; writing books or articles on information security, or volunteering for (ISC)². Full information on CPE requirements is made available to CISSPs after certification.

Systems Security Certified Practitioner (SSCP)

The Systems Security Certified Practitioner certification is intended for information security practitioners who have at least one year of experience in one or more of the seven information security domains tested in the SSCP examination. Unlike the CISSP designation which is a professional-level qualification SSCP is a practitioner-level qualification; this fact is reflected in the content and length of the examination and experience requirements. SSCP candidates are examined for a working knowledge of the following seven domains of the Common Body of Knowledge:

- Access Controls
- Administration
- Audit and Monitoring
- Cryptography
- Data Communications
- Malicious Code/Malware
- Risk, Response and Recovery

The SSCP examination consists of 125 multiple-choice questions to be answered in 3 hours. The examination is available at all sites where (ISC)^2 examinations are conducted. The registration fee for the examination is US$ 350. (ISC)^2 review seminars are available from the (ISC)^2 Institute; additionally a number of training companies offer SSCP preparation courses. As with other (ISC)^2 qualifications an official study guide is available from the (ISC)^2. In addition to a passing score candidates will have to subscribe to the (ISC)^2 Code of Ethics and provide proof of at least one year of information security work experience in one or more of the seven domains. Systems Security Certified Practitioners are required to earn 60 hours of continuing professional education (CPE) credits every three years to keep their certification in good standing. An annual maintenance fee of US$ 65 is also payable. Upon completion of all requirements for the SSCP designation a certificate and an SSCP ID card are issued. SSCPs also have the right to participate in annual (ISC)^2 elections.

(ISC)² Associate

Announced in 2003 the (ISC)² Associate qualification is intended for newcomers to the information security profession who do not yet satisfy the requirements for a CISSP or SSCP designation. The goal of the (ISC)² Associate qualification is to support them on their qualification path towards CISSP or SSCP and provide an interim assessment of their knowledge.

Candidates may register for and take the CISSP or SSCP examination and upon successful completion become (ISC)² Associates. When or if they accumulate the required work experience and provide a completed endorsement form to the (ISC)² they will be granted the CISSP or SSCP designation. The (ISC)² Associate status is valid for five years and the Associate has to fulfil the requirements for the CISSP or SSCP designation during these five years.

It is necessary to note that (ISC)² Associates are not certified by (ISC)² as information security professionals and may not represent themselves as such. An annual maintenance fee of US$ 35 applies to (ISC)² Associates and must be paid in order to maintain the Associate status. Continuing professional education (CPE) requirements do not apply to (ISC)² Associates.

Information Systems Security Architecture Professional (ISSAP)

Certified Information Systems Security Professionals in good standing may wish to obtain one or more of the available CISSP concentrations to prove a higher level of mastery of either Security Architecture, Security Management or Security Engineering than those required of CISSPs. The Information Systems Security Architecture Professional (ISSAP) designation is intended for CISSPs who can demonstrate expert-level competence in the following information security domains:

- Access control systems and methodologies
- Telecommunications and network security
- Cryptography
- Requirements analysis & security standards, guidelines, and criteria
- Technology-related business continuity planning and disaster recovery planning

The ISSAP examination consists of 100 scored plus 25 pretest items – for a total of 125 questions to be completed in three (3) hours. At the time of writing the examination fee is US$ 295 and the annual maintenance fee is US$ 35 (in addition to the CISSP annual maintenance fee). Additionally, 20 of the required 120 continuing professional education (CPE) units must be earned in the area of specialisation (architecture). The ISSAP examination is available at all (ISC)^2 examination sessions. An official study guide for the ISSAP concentration is available online from the (ISC)^2 at www.isc2.org. Training for ISSAP is expected to be available in 2004.

Information Systems Security Management Professional (ISSMP)

The Information Systems Security Management Professional concentration is for Information security managers holding the CISSP designation who would like to demonstrate more in-depth specialisation in information security management. The ISSMP concentration covers the following information security domains:

- Enterprise security management practices
- Enterprise-wide system development security
- Overseeing compliance of operations security
- Understanding business continuity and disaster recovery planning
- Law, investigations, forensics and ethics

Like the ISSAP concentration examination, the ISSMP examination consists of 100 scored plus 25 pretest items – for a total of 125 questions to be completed in three (3) hours. At the time of writing the examination fee is US$ 295 and the annual maintenance fee is US$ 35 (in addition to the CISSP annual maintenance fee). Additionally, 20 of the required 120 continuing professional education (CPE) units must be earned in the area of specialisation (management). The ISSMP examination is available at all (ISC)^2 examination sessions. An official study guide for the ISSMP concentration is available online from the (ISC)^2 at www.isc2.org. Training for ISSMP is expected to be available in 2004.

Information Systems Security Engineering Professional (ISSEP)

The Information Systems Security Engineering concentration was developed jointly by the International Information Systems Security Certification Consortium and the Information Assurance Directorate of the U.S. National Security Agency (NSA) under the U.S. Federal Technology Transfer Act of 1986. As such, the ISSEP concentration is mostly relevant to U.S.-based information security professionals. In future ISSEP-certified professionals will be required or preferred by the National Security Agency for certain information security projects. The information security domains examined for the ISSEP designation are the following:

- Systems security engineering
- Certification and accreditation
- Technical management
- U.S. Government Information Assurance Regulations

Unlike the ISSAP and ISSMP concentrations the ISSEP examination consists of 125 scored and 25 pre-test questions, for a total of 150 questions to be completed in 3 hours. Other requirements – such as exam fees, annual maintenance fees and required continuing professional education credits – are the same as for ISSAP and ISSMP concentrations. The Official ISSEP Study Guide is available online from the (ISC)^2 at www.isc2.org.