2003

ISQ Handbook

An in-depth coverage of vendor and vendor-neutral qualifications

Information

Security

Qualifications

ISN

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Contents

Preface

Increasing computerization of government infrastructures has given rise to new vulnerabilities and challenges. Information Technologies (IT) have improved workflow efficiency, while exposing governments to new threats, which challenge not only national security, but also socio-economic development. Certain technologies deliver powerful weapons that can be used for new forms of warfare and cyber crime, undermining the availability and integrity of reliable and confidential information vital for the continuity of government services. The International Relations and Security Network (ISN) has launched a new training program to strengthen the information security skills of government professionals throughout the Euro-Atlantic region, to cope with these threats and to develop information protection mechanisms. The seminar curricula are designed to raise EAPC/PfP defense policy makers' awareness of the existing and emerging information security risks, and to develop information security specialists' skills to guarantee the maximum possible security of national information systems.

The current publication is a follow-up to the first ISN Partnership for Peace (PfP) Seminar on Information Security held at the ETH Zurich (Swiss Federal Institute of Technology) in August 2003 as an effort to further a more consistent and formally structured education and training of the EAPC/PfP professionals in the field of information security. In today's networked environment, there is a considerable need for hands-on and professional education in information security throughout the Euro-Atlantic Partnership Council region. A wide range of non-profit and commercial organizations offer information security training and qualifications. A careful selection from globally available training tools and products matching the professionals' organizational needs and local conditions is key to sustainable information security education.

The objective of the ISN Information Security Qualifications Handbook is to deepen the understanding of EAPC/PfP information security specialists on the existing range of information security qualifications and facilitate a professional selection of appropriate training programs supporting their specific job responsibilities and organizational priorities. For this reason, the Handbook covers in depth two types of information security qualifications: vendor neutral and vendor qualifications.

The Handbook has been developed in cooperation with Danielyan Consulting LLP, an Information Security consultancy and an ISN Cooperating Partner. Special thanks go to Danielyan Consulting LLP for its stocktaking work and for sharing its first-hand experience with the information security professionals in the EAPC/PfP community.

We very much hope that the ISN Information Security Qualifications Handbook will serve as a reference book for the interested community. The publication forms an integral part of the ISN's commitment to promote and enhance information security through training and education within the framework of Switzerland's commitment to fighting asymmetric threats throughout the Euro-Atlantic Partnership Council region.

Zurich, November 2003

Anna Hess Sargsyan
Partnership for Peace Training Coordinator
International Relations and Security Network

Introduction

The objective of this publication is to introduce existing practical information security qualifications and serve as an easy-to-use reference for both prospective students of information security and their organisations. Developed by Danielyan Consulting LLP, an information security consultancy, at the request of the International Relations and Security Network (ISN) at the Swiss Federal Institute of Technology Zurich, this publication aims to continue and contribute to ISN's training activities in the information security field launched by the ISN Information Security Fundamentals seminar held in Zurich on 25–27 August 2003.

Unlike most other arts and sciences, where established institutions of higher education are usually the primary or even the only source of education and training, information security as a relatively new discipline at the crossroads of diverse, yet equally important subjects such as cryptography, electrical engineering, computer science and law does not enjoy, for better or for worse, such a situation. What we have now in the information security profession is a number of different organisations, both non-profit and commercial, offering information security training and qualifications. While some traditional higher education institutions are now offering degrees and certificate programs in information security, most of them are usually theoretical in nature and do not prepare the students for a practical information security work at their organisations. As a result, non-academic – professional and/or practitioner – qualifications coupled with relevant work experience offer more in terms of readily usable skills and knowledge than most academic venues of study.

Naturally, not all training and qualification programs are created equal – aside from the obvious differences in specialisation, focus and professional level, they also differ in aspects such as costs and recognition, so it is not easy to choose the most appropriate and rewarding qualification to pursue. For an IT specialist, to gather the necessary details and understand all the pros and cons of all available qualifications and choose the one which is the most appropriate given their experience, prior knowledge, job responsibilities and career goals, is a considerable task. The aim of the ISN Information Security Qualifications Handbook is to guide and assist in this matter.

For the purposes of this handbook information security qualifications are grouped into two broad categories: vendor-neutral (presented in Part One) and vendor qualifications (introduced in Part Two of this handbook).

By definition vendor-neutral qualifications focus on universal information security principles, skills and knowledge, which do not depend on particular system, solution, or IT environment. Vendor qualifications, in contrast, mainly offer in-depth coverage of particular vendor's products and solutions and focus less on general information security concepts and knowledge than vendor-neutral qualifications. Vendor qualifications may be seen as specialisations which may be pursued, if appropriate, after gaining a vendor-neutral qualification in information security. In this case general information security skills and knowledge would be complemented by the in-depth mastery of the particular vendor's solutions.

All in all, 81 qualifications awarded by 29 organisations are covered in this handbook, of which 45 qualifications are vendor-neutral and 36 are vendor qualifications.

I hope this publication will be of assistance to those interested in information security studies and will contribute to the security and reliability of our societies' information systems and infrastructures.

Edgar Danielyan
Danielyan Consulting LLP

Comparison of vendor-neutral general information security qualifications

Qualification	Awarded by	Approx. level	Requirements	CPE	Cost *
Security+	CompTIA	Entry-level	Examination	No	US$ 225
TICSA	TruSecure	Entry-level	Examination and work experience or approved training	Yes	US$ 395
CIWSP	CIW	Entry-level	Two examinations	No	US$ 320
GISF	GIAC	Entry-level	Two examinations and practical assignment	Yes	US$ 250 + training
(ISC)^2 Associate	(ISC)^2	Practitioner	Examination and subscription to code of ethics	No	US$ 369 or US$ 499
GSEC	GIAC	Practitioner	Two examinations and practical assignment	Yes	US$ 450
SSCP	(ISC)^2	Practitioner	• Examination • Subscription to code of ethics • Minimum 1 year of work experience	Yes	US$ 369
SCNP	SC	Practitioner	Two examinations	No	US$ 300
CIWSA	CIW	Practitioner	Minimum three examinations	No	US$ 320 + variable
CISSP	(ISC)^2	Professional	Examination Subscription to code of ethics Minimum 4 years of work experience Professional sponsorship and verification	Yes	US$ 499
SCNA	SC	Professional	Four examinations	No	US$ 330
CISA	ISACA	Professional	• Examination • Subscription to code of ethics • Professional sponsorship and verification • Minimum 5 years of work experience	Yes	US$ 495
CISM	ISACA	Professional	• Examination • Subscription to code of ethics • Professional sponsorship and verification • Minimum 5 years of work experience	Yes	US$ 495
GSE	GIAC	Professional	Number of requirements – please see the entry for GSE	Yes	US$ 2,250

* Please note that costs depend on candidate's circumstances (such as examination location, membership and so on), do not include preparation, training or travel expenses, and are subject to change. For up to date information please contact the awarding organisation.

CPE = Continuing Professional Education requirements

Vendor-neutral general information security qualifications by level

Entry-level qualifications

- CompTIA Security+
- TruSecure ICSA Certified Security Associate
- CIW Security Professional
- GIAC Information Security Fundamentals

Practitioner qualifications

- (ISC)^2 Associate
- GIAC Security Essentials Certification
- Systems Security Certified Practitioner
- Security Certified Network Professional
- CIW Security Analyst

Professional qualifications

- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- Certified Information Security Manager
- GIAC Security Engineer
- Security Certified Network Architect

Vendor-neutral information security qualifications by specialisation

Architecture:	ISSAP
Management:	CISSP, ISSMP, GSLC, CISM, CISMP
Engineering:	ISSEP, GSE
Firewalls:	GCFW
Intrusion detection:	GCIA
Incident handling:	GCIH, CERT
Audit:	GSNA, CISA, GSAE, BS7799 LA, BS7799 IA
Forensics:	GCFA, CCFT, CIFI, CFCE
Physical security:	CPP, PSP
Investigations:	PCI, CCCI, CCCP, CCCA, CIFI
Business continuity:	ABCP, CBCP, MBCP
Fraud:	CFE

Testing organisations

Examinations mentioned in this handbook are either administered by the awarding bodies themselves (sometimes with the assistance of specialised testing and knowledge measurement advisors), or by one or both of the following two worldwide testing organisations:

Pearson VUE (www.vue.com)

Pearson Virtual University Enterprises (VUE) is a part of the Pearson Group. VUE administers both professional licensure and information technology certification examinations. Visit www.vue.com for more information on examination fees, testing centre locations and list of offered examinations. Online exam registration and payment available.

Thomson Prometric (www.prometric.com)

Thomson Prometric is a subsidiary of Thomson Corporation and has testing centres in over 120 countries around the world. Prometric provides professional and academic examination services in addition to IT certification examinations. Visit www.prometric.com for more information on examination fees, testing centre locations and list of offered examinations. Online exam registration and payment available.

Form of examinations

All examinations administered by VUE and Prometric use computer-based testing (CBT) technology. Examinations administered by awarding bodies themselves may take form of either computer-based testing or pen and paper examinations.

Part I

Vendor Neutral Qualifications

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.

Global Information Assurance Certification (GIAC)

Website:	www.giac.org
E-mail:	info@giac.org
Address:	5401 Westbard Avenue, Suite 1501 Bethesda, MD 20816, USA
Phone:	+1 540 548 0977
Fax:	+1 540 548 0957

Established in 1999 by the System Administration, Audit, Networking and Security (SANS) Institute (www.sans.org), the Global Information Assurance Certification programme is quickly gaining support and recognition due to its high quality curriculum, training and certifications. Enjoying support of some of the best professionals in the industry and academia the Global Information Assurance Certification is now on par with such long-standing and veteran organisations as the International Information Systems Security Certification Consortium and the Information Systems Audit and Control Association. GIAC offers numerous qualifications at levels ranging from novice to expert in different specialisations such as information security management, UNIX, Windows, audit, incident handling, forensics and others.

One of the certification requirements which sets GIAC qualifications apart from others is the requirement to complete written practical assignments before taking the examinations – which is intended to demonstrate candidates' ability to apply their skills in practice. Other GIAC-specific requirement is the practice of online examinations which are conducted over the Internet – whereas other qualifications require candidates to visit either Prometric or VUE testing centres or attend specially arranged examination sessions to sit their exams.

GIAC qualifications are available as tuition plus exam offerings from the SANS Institute (both online and face to face tuition is available) or as so called "challenge" examinations for those who believe they have the required skills and knowledge to take on the exam without much study.

GIAC qualifications also need to be regularly renewed to ensure that certification holders still meet the certification criteria.

GIAC Security Essentials Certification (GSEC)

The GSEC is a general foundation level certification for anyone responsible for security. GSEC is a practical qualification, like other GIAC qualifications; GSEC holders are expected to have the required skills, knowledge and abilities to understand principles of information security and implement information security solutions. The GIAC Security Essentials Certification covers the following subjects:

- Risk assessment and auditing
- Host and network based intrusion detection
- Honeypots, firewalls and perimeter protection
- Security policy
- Password management
- Security incident handling
- Information warfare
- Web security
- Network fundamentals and IP concepts
- Cisco router filters
- Primary threats for perimeter protection
- PGP, steganography
- Anti-viral tools
- Windows security administration and auditing
- IIS security
- Unix security fundamentals

GIAC costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more detailed information on GIAC Security Essentials Certification please visit GIAC at www.giac.org.

GIAC Certified Firewall Analyst (GCFW)

GIAC Certified Firewall Analyst is an intermediate level qualification for those network security professionals who specialise in design, implementation, configuration and monitoring of firewalls. Recertification is required every four years. The following subjects are covered by GCFW training and certification programme:

- IP stimulus/response and fragmentation
- Complex IP transports and services
- Tcpdump, Windump, Ethereal and other sniffers
- Business needs vs. security
- Static packet filtering
- Stateful packet filtering and inspection
- Proxies
- In-depth coverage of popular firewall products
- Implementing security with Cisco routers
- Intrusion detection
- Centralized logging
- Firewall log file analysis
- Log file alerting
- IPSec, SSL, and SSH
- Designing a secure perimeter
- Network and host based auditing

GCFW costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more information on GCFW please visit GIAC at www.giac.org.

GIAC Certified Intrusion Analyst (GCIA)

GCIA is an intermediate qualification aimed at intrusion detection specialists who configure, maintain and monitor intrusion detection systems and need to read and analyse network traffic and related logs. GCIA certification needs to be renewed every four years and covers the following subjects:

- TCP/IP fragmentation
- ICMP
- Microsoft networking and security
- Client and server Interaction
- Routing
- IPSec
- Tcpdump
- General network traffic analysis
- Snort
- Snort rules
- Intrusion detection architecture
- Intrusion detection analysis
- Traffic and external analysis

GCIA certification costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more information on GCIA certification and training please visit GIAC at www.giac.org.

GIAC Certified Incident Handler (GCIH)

GCIH certification is an intermediate level qualification for those who are responsible for incident handling and response within larger security teams. GCIH certification needs to be renewed every two years and covers the following topics:

- The step-by-step approach used by attackers
- The latest computer attack vectors
- Proactive and reactive defences for each stage of a computer attack
- Scanning for, exploiting and defending systems
- Strategies and tools for detecting each type of attack
- Attacks and defences for Windows, UNIX, switches, routers and other systems
- Application-level vulnerabilities, attacks and defences
- Developing an incident handling process
- Legal issues in incident handling
- Recovering from computer attacks and restoring systems for business

GCIH costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

More details on the GCIH certification is available from www.giac.org.

GIAC Certified Windows Security Administrator (GCWN)

An intermediate qualification, GCWN is specifically targeted at Windows (XP, 2000, and NT) administrators who are responsible for security on Windows networks. This certification must be renewed every two years to keep holders updated on latest challenges and solutions. The following topics are covered in particular:

- Active Directory design
- Delegation of authority
- Dynamic DNS
- Group policy design
- Security templates
- PKI installation and management
- Encrypting file system
- Smart cards and tokens
- IP Security Architecture
- Virtual private networking
- Routing and remote access service
- IIS authentication and authorization
- IIS ISAPI extensions and filters
- Windows scripting
- Scripting: ADSI, CDO, WMI

GCWN costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For up to date information on GCWN please visit www.giac.org.

GIAC Certified UNIX Security Administrator (GCUX)

GIAC Certified UNIX Security Administrator is an intermediate general UNIX security qualification targeted at UNIX system and network administrators who want better and deeper understanding of UNIX security issues and technologies. GCUX needs to be renewed every two years and covers the following topics:

- Passwords and alternatives
- Memory attacks and overflows
- Trojan horse programs
- Network-based attacks
- Physical security
- Security scanners
- Passwords and privilege
- Network security
- Secure Shell
- UNIX forensics
- Common issues with users and management
- Network Time Protocol
- BIND installation and configuration
- Sendmail security
- Linux specifics
- Solaris specifics
- Logging

GCUX costs are as follows:

With SANS online training	US$ 250 + training
With SANS conference training	US$ 250 + training
Challenge (examination only)	US$ 450

For more information on GCUX training and certification please visit GIAC at www.giac.org.

GIAC Information Security Fundamentals (GISF)

Set at an introductory level the GIAC Information Security Fundamentals certification is aimed at candidates who would like to acquire overall understanding of information security risks, considerations and solutions. To obtain the GISF certification candidates will have to pass two examinations and complete a practical assignment. The GISF designation needs to be renewed every two years and covers the following subjects:

- Understanding information security threats and risks
- Identifying best practices
- Risk management
- Security management
- Access controls, attacks and countermeasures
- Secrecy and privacy
- Auditing concepts
- Internet Protocol
- Routing
- Domain Name Service
- Security considerations
- Basics of cryptography
- Defence in depth

GISF certification costs are as follows:

With SANS online training	US$ 250
With SANS conference training	US$ 250

GISF examination without SANS training is not yet available – please visit www.giac.org for up to date information on availability.

GIAC Systems and Network Auditor (GSNA)

GSNA is an intermediate-level qualification for systems and networks auditors. It must be renewed every two years and covers the following subjects:

- Top 20 vulnerabilities
- Forensic techniques
- Firewall and perimeter auditing
- Audit process
- Time based security
- Blending audit objectives with corporate policy
- Before an incident occurs
- Rootkit pathology
- Uncovering “back doors”
- Building a forensics toolkit
- Detailed audit of a router
- Network security
- Password harvesting
- Nmap
- Network mapping
- Analyzing the results
- Security committees
- Audit tools
- Windows auditing
- UNIX auditing

GSNA costs are as follows:

With SANS conference training	US$ 250

SANS online training and challenge only examination are not yet available for GSNA; please check www.giac.org for up to date information on availability.

GIAC Certified Forensic Analyst (GCFA)

For information security professionals who are responsible for forensic investigation and/or analysis, advanced incident handling, or formal incident investigation the Global Information Assurance Certification programme offers the GIAC Certified Forensic Analyst intermediate-level qualification which covers the following subjects:

- Incident response
- Forensic preparation
- Windows forensics
- UNIX forensics
- Data recovery and analysis
- Malicious code analysis
- Law enforcement interaction and case law
- Corporate and managerial legal concerns and direction
- The Honeynet project's forensic challenge

GCFA certification must be renewed every four years; GCFA costs are as follows:

With SANS conference training	US$ 250

SANS online training and challenge only examination are not yet available for GCFA; please visit www.giac.org for up to date information on GCFA training and examination availability.

GIAC IT Security Audit Essentials (GSAE)

The GIAC IT Security Audit Essentials certification is appropriate for those new to IT security audit. It is a foundation level qualification with recertification requirement of every two years and covers the following topics:

- Host- and network-based intrusion detection
- Firewalls and honeypots
- Vulnerability scanners
- Computer security policies
- Password management
- Incident handling
- Information warfare
- Encryption
- Steganography
- Virtual private networks
- Public key infrastructures

GSAE costs are as follows:

With SANS conference training	US$ 250

SANS online training and challenge only examination are not yet available for the GSAE certification; please visit www.giac.org for up to date information on availability.

GIAC Security Leadership Certificate (GSLC)

The GIAC Security Leadership Certificate is the GIAC's certification for managers who would like to learn the essential, up to date knowledge and skills required to manage information security component of IT projects.

- Risk assessment and auditing
- Host and network based intrusion detection
- Honeypots, firewalls and perimeter protection
- Security policy
- Password management
- Security incident handling
- Information warfare
- Web security
- Network fundamentals
- IP concepts and behaviour
- Cisco router filters
- Primary threats for perimeter protection
- PGP, steganography
- Anti-viral tools

GSLC costs are as follows:

With SANS conference training	US$ 250

GSLC online training and challenge only examination are not available. Please visit www.giac.org for up to date information on training and examination availability.

GIAC Gold Standard Certificate (GGSC)

Two GIAC Gold Standard Certificates are currently available:

- GIAC Solaris Gold Standard Certificate
- GIAC Windows 2000 Gold Standard Certificate

These certificates are for system and network administrators who manage Solaris 8/9 and Windows 2000 systems and networks and are based on "gold standards" defined by the Center for Internet Security (CIS) benchmarks.

These certifications are free of charge when taken with SANS conference training; certification with SANS online training is US$ 100; and only GIAC Solaris Gold Standard Certificate is available as a challenge only examination for US$ 250.

For more information on Gold Standard Certificates and their availability please visit www.giac.org.

GIAC Security Engineer (GSE)

The GIAC Security Engineer certification is the most advanced information security qualification awarded by the Global Information Assurance Certification programme. To earn this highly respected professional designation candidates are required to have five (5) GIAC subject area certifications:

- GIAC Certified Firewall Analyst
- GIAC Certified Intrusion Analyst
- GIAC Certified Incident Handler
- GIAC Certified Windows Security Administrator
- GIAC Certified UNIX Security Administrator

Additionally, other requirements (examination, presentation and an on-site security evaluation) must be met. As of November 2003, only two individuals have earned GIAC's highest professional designation: Mr John Jenkinson, GSE, and Mr Lenny Zeltser, GSE. For up to date information on the GSE designation please visit GIAC at www.giac.org.

Computing Technology Industry Association (CompTIA)

Website:	www.comptia.org
Address:	1815 S. Meyers Road, Suite 300 Oakbrook Terrace, IL 60181-5228, USA
Phone:	+1 630 678 8300
Fax:	+1 630 268 1384

The Computing Technology Industry Association has more than 16,000 members in more than 89 countries. As a leading trade association it works to advance industry growth, advance public policy on information technology and develop vendor-neutral IT certifications. To date 600,000 IT professionals worldwide have achieved CompTIA certifications. One of the most widely know CompTIA certifications is CompTIA A+.

In 2002, the CompTIA announced a new foundation-level certification: CompTIA Security+. The Security+ certification is aimed at IT professionals such as system and network administrators with up to two years work experience who are not security professionals per se but who have certain security responsibilities and would benefit from a security qualification. Among organisations who recognise Security+ are:

- U.S. Federal Bureau of Investigation
- IBM
- Microsoft
- Motorola
- Novell
- RSA Security
- Sun Microsystems
- VeriSign
- U.S. Secret Service
- Information Systems Audit and Control Association

CompTIA Security+

The CompTIA Security+ certification is appropriate for IT professionals who are new to the information security profession. Ideal candidates for Security+ certification are system and network administrators, senior help desk personnel, and other IT professionals whose core job function is not security but who would benefit from a foundation-level security qualification. Although not required, it is recommended that Security+ candidates already hold CompTIA Network+ or comparable certification.

To obtain the Security+ certification candidates need to take and pass the computerised multiple-choice Security+ exam at any Prometric or VUE testing centre worldwide. The examination is 100 questions long and is to be completed in 90 minutes. The content of the examination is divided into five domains as follows:

1. General security concepts	30%
2. Communications security	20%
3. Infrastructure security	20%
4. Basics of cryptography	15%
5. Operational/organisational security	15%

The passing score is 764 graded on a scale of 100–900. As with other Prometric/VUE examinations the score is calculated and displayed immediately at the end of the examination session. The examination fee is variable and depends on the location of the testing centre, number of booked exams and CompTIA membership status of candidates. The average examination fee is US$ 200.

Training for the CompTIA Security+ qualification is available in many forms from a number of training providers. Self-learning options include certification guides and computer-based training solutions; instructor-led courses include both face to face and online tuition. For more detailed information on Security+ and available training please visit CompTIA at www.comptia.org.

TruSecure Corporation

Website:	www.trusecure.com
E-mail:	info@trusecure.com
Address:	13650 Dulles Technology Drive
	Herndon, VA 20171, USA
Phone:	+1 703 480 8200

The TruSecure Corporation is one of the most well-known information security solutions providers. Through its independent division, ICSA Laboratories, it also operates one of the leading product certification programmes, certifying anti-virus, firewall, IPSEC, cryptography and other information security products.

In 2002, TruSecure Corporation entered the information security qualifications field by introducing the TruSecure ICSA Certified Security Associate (TICSA) certification – a vendor-neutral, skills-based, pragmatic foundation-level qualification.

TruSecure ICSA Certified Security Associate (TICSA)

The TruSecure ICSA Certified Security Associate qualification is designed to validate IT security skills of network and system administrators, audit personnel, and other IT professionals. This qualification has the status of a "CISSP Complementary Certification" as announced by the International Information Systems Security Certification Consortium.

TICSA requirements for certification include the following: at least 2 years experience in network security administration or at least 48 hours of approved computer security training within the last 24-month period; subscription to a Code of Ethics; completion of a practitioner's profile; and a passing score on the TICSA exam. TruSecure Essential Body of Knowledge includes the following 14 domains which are tested in the examination:

- Essential security practices
- Risk management fundamentals
- Malicious code threats and common defensive mechanisms
- Firewall architectures, properties, and administration
- Intrusion detection, response and recovery
- Administrative maintenance and change control issues
- System/network design configuration and fundamentals
- TCP/IP networking basics
- Law, ethics and policy issues
- Authentication processes and techniques
- Cryptography basics
- Host and network security fundamentals
- PKI and digital certificates basics
- Operating system security fundamentals

The TICSA examination is available at all Prometric testing centres worldwide and consists of 70 multiple-choice questions. Examination fees depend on the testing centre location and are around US$ 200. TICSA certification is valid for two years; continuing professional education requirements apply and may be satisfied by attending information security training courses, seminars and conferences. Training for the TICSA qualification includes self-study guides and training courses. A list of current training providers and resources is available online from www.trusecure.com.

Security Certified Program (SCP)

Website:	www.securitycertified.net
E-mail:	info@securitycertified.net
Address:	825 West State Street, Suite 204 Geneva IL 60134, USA
Phone:	+1 630 208 5030
Fax:	+1 630 208 4807

The Security Certified Program is run by Ascendant Learning LLC, a training provider based in Illinois, USA. The program includes two qualifications: Security Certified Network Professional (SCNP) and Security Certified Network Architect (SCNA). Each qualification involves passing two associated examinations which are available from both Prometric and VUE testing centres. SCP authorised training providers teach the SCP curriculum in 36 countries around the world. Before embarking on study for the Security Certified Network Professional (SCNP) qualification candidates are recommended to have CompTIA Security+ certification, although this is not a requirement. SCNP is a requirement which must be satisfied before proceeding to the Security Certified Network Architect (SCNA) examination.

Security Certified Network Professional (SCNP)

The Security Certified Network Professional focuses on two important aspects of network security: firewalls and intrusion detection. The recommended prerequisite for the SCNP certification is CompTIA Security+ or comparable experience. SCNP includes two examinations, “Hardening the infrastructure” and “Network defence and countermeasures” with the following objectives:

Hardening the infrastructure (6 domains)

1. Contingency planning	5%
2.Tools and techniques	9%
3.Internet and WWW security	11%
4. Router security and ACLs	15%
5.TCP/IP packet structure and security	25%
6.Operating system security	35%

Network defence and countermeasures (6 domains)

1. Network defence fundamentals	5%
2.Security policy design and implementation	10%
3.Network traffic signatures	10%
4. VPN concepts and implementation	15%
5.IDS concepts and implementation	30%
6.Firewall concepts and implementation	30%

SCNP examination fees are US$ 150 per exam; the examinations are available at Prometric and VUE testing centres. Both Ascendant Learning and third-party training providers offer SCNP training.

Security Certified Network Architect (SCNA)

Like the SCNP the Security Certified Network Architect designation requires passing scores on two associated examinations; however, unlike SCNP, SCNA is a more advanced qualification which builds upon the foundation laid by SCNP. The two exams required for SCNA are “Enterprise security implementation” and “The solution exam”:

Enterprise security implementation (9 domains)

1. Law and legislation	5%
2. Forensics	7%
3. Wireless security	7%
4. Secure e-mail	8%
5. Biometrics	8%
6. PKI policy and architecture	10%
7. Digital certificates and digital signatures	15%
8. Cryptography	20%
9. Strong authentication	20%

The solution exam

The solution exam is a case scenario-type examination which requires comprehensive understanding of all issues and technologies examined in the two SCNP exams and the “Enterprise security implementation” exam. Although the solution exam is in the multiple-choice format its questions and answers are considerably longer and are more complex in order to reflect the complexity of decisions faced by network architects.

Both SCNA examinations cost US$ 180 per exam and are available at Prometric and VUE testing centres like the SCNP examinations. Training for the SCNA is also available from Ascendant Learning and third-party training providers.

International Council of E-Commerce Consultants (EC-Council)

Website:	www.eccouncil.org
E-mail:	info@eccouncil.org
Address:	67 Wall Street, 22nd Floor New York, NY 10005-3198, USA
Phone:	+1 212 709 8253
Fax:	+1 212 943 2300

The mission of the International Council of E-Commerce Consultants is to foster development of e-commerce, provide education and certification, set professional standards and stimulate the growth of e-commerce through open dialogue and exchange of ideas.

Based in New York City the EC-Council offers several e-commerce qualifications, including the Certified Ethical Hacker (CEH) designation.

Certified Ethical Hacker (CEH)

“*To catch a thief, you must think like a thief. To protect your network from a hacker, you’ve got to get inside that hacker’s mind.*” This is the idea behind the Certified Ethical Hacker (CEH) qualification from the International Council of E-Commerce Consultants. To some in the information security profession the CEH designation is controversial – and not only because of the H-word in the qualification title – it may be seen as an oxymoron – but also because of perceived insufficiency of accent on ethics in the curriculum and exam objectives. Whether this is the case or not is open to debate.

To achieve the CEH designation candidates need to take and pass the CEH examination consisting of 50 multiple-choice questions to be answered in 2 hours; the passing score is 70%. The exam is available at Prometric testing centres. The subjects examined on the examination are as follows:

- Ethics and Legal Issues
- Footprinting
- Scanning
- Enumeration
- System Hacking
- Trojans and Backdoors
- Sniffers
- Denial of Service
- Social Engineering
- Session Hijacking
- Hacking Web Servers
- Web Application Vulnerabilities
- Web Based Password Cracking Techniques
- SQL Injection
- Hacking Wireless Networks
- Virus and Worms
- Hacking Novell
- Hacking Linux
- IDS, Firewalls and Honeypots
- Buffer Overflows
- Cryptography

Training for the CEH designation is available from both the EC-Council and other training providers. The CEH examination may be taken at Prometric testing centres.

CIW

Website:	www.ciwcertified.com
Address:	410 N. 44th Street, Suite 600 Phoenix, AZ 85008, USA
Phone:	+1 602 794 4199
Fax:	+1 602 794 4198

Originally aimed at webmasters the CIW certifications and training have outgrown that specialisation and currently offer certification and training in many information technology areas, including security. There are more than 800 CIW authorised training providers in 64 countries. CIW training and certifications are recognised by Intel, Novell, IBM and Hewlett-Packard among others.

CIW offers two security qualifications – CIW Security Professional and CIW Security Analyst.

CIW Security Professional

The CIW Security Professional is an entry-level certification and covers the following three areas:

1. Network security and firewalls	22 questions
2.Operating systems security	16 questions
3 Security auditing, attacks and threat analysis	22 questions
Total number of exam questions	60

The prerequisites for the CIW Security Professional designation are the CIW Certification Agreement and the CIW Associate certification. Only individuals who hold the CIW Associate certification may register for and attempt the CIW Security Professional examination. The examination itself consists of 60 multiple-choice questions and is to be completed in 75 minutes. Both Prometric and VUE testing centres offer CIW examinations. Training for the CIW Security Professional designation is available in self-study and instructor-led forms.

CIW Security Analyst

CIW Security Professionals who also hold any one of the following qualifications may apply for the CIW Security Analyst designation:

- Microsoft Certified Systems Administrator (MCSA)
- Microsoft Certified Systems Engineer (MCSE) NT 4
- Microsoft Certified Systems Engineer (MCSE) 2000
- Certified Novell Engineer (CNE) 4
- Certified Novell Engineer (CNE) 5
- Cisco Certified Network Professional (CCNP)
- Cisco Certified Network Associate (CCNA)
- Cisco Certified Internetwork Expert (CCIE)
- Linux Professional Institute (LPI) Level 2
- SAIR Level 2 LCE

CIW Security Analyst designation is a proof of both general computer security knowledge examined in CIW Security Professional examination and vendor-specific skills examined under particular vendor's certification programme. CIW Security Analyst certification may be considered a practitioner-level qualification.

Information Systems Audit and Control Association (ISACA)

Website:	www.isaca.org
Address:	3701 Algonquin Road, Suite 1010
	Rolling Meadows, IL 60008, USA
Phone:	+1 847 253 1545
Fax:	+1 847 253 1443

Founded in 1969 as the EDP Auditors Association, today the Information Systems Audit and Control Association with its 28,000 members in more than 100 countries sets standards for information systems audit, control and governance. With local and regional chapters in more than 60 countries ISACA is also active at the local level; ISACA-sponsored conferences are regularly held in North America, Europe, and Asia.

The Information Systems Audit and Control Association offers two respected professional information security qualifications: the long-standing Certified Information Systems Auditor (CISA) and the new Certified Information Security Manager (CISM) designations.

Certified Information Systems Auditor (CISA)

The Certified Information Systems Auditor designation is a professional-level qualification awarded to experienced information systems audit, control and security professionals who have met the following requirements for certification:

- Successful completion of the CISA examination
- Minimum five years of information systems auditing, control or security experience
- Adherence to the Code of Professional Ethics
- Adherence to the continuing professional education requirements
- Compliance with the Information Systems Auditing Standards promulgated by the ISACA

The CISA examination is held once a year in many locations worldwide. It consists of 200 multiple-choice questions to be answered in 4 hours and covers the following seven domains:

1.	Management, planning and organisation of IS	11%
2.	Technical infrastructure and operational practices	13%
3.	Protection of information assets	25%
4.	Disaster recovery and business continuity	10%
5.	Application development, acquisition and implementation	16%
6.	Business process evaluation and risk management	15%
7.	The information systems audit process	10%

Minimum five years of verified professional experience in auditing, control or security is required in addition to a passing score on the CISA examination. Certified Information Systems Auditors are also required to comply with strict continuing professional education requirements and comply with the Information Systems Auditing Standards promulgated by ISACA. Examination fee for the CISA examination depends on the time of registration and the ISACA membership status of the candidate and ranges from US$ 295 to US$ 495. CISA preparation materials are available from the Association and third-party providers.

Certified Information Security Manager (CISM)

Certified Information Security Manager is a new professional-level qualification from the Information Systems Audit and Control Association. Aimed specifically at information security managers the CISM examination covers five domains:

1. Information security governance	21%
2. Risk management	21%
3. Information security programme management	21%
4. Information security management	24%
5. Response management	13%

In addition to the successful completion of the CISM examination candidates are required to have at least five years of professional information security management experience and commit themselves to continuing professional development requirements and code of ethics. Certified Information Systems Security Professionals (CISSPs) and Certified Information Systems Auditors (CISAs) are entitled to two years work experience waiver when applying for the CISM designation.

For up to date information on CISM please visit Information Systems Audit and Control Association online at www.isaca.org.

British Standards Institute

Website:	www.bsi-global.com
E-mail:	cservices@bsi-global.com
Address:	389 Chiswick High Road London W4 4AL, United Kingdom
Phone:	+44 20 8996 9000
Fax:	+44 20 8996 7001

The British Standards Institute, founded in 1901, has more than 5,000 employees in 110 countries worldwide and works in the following areas:

- Independent certification of management systems and products
- Commodity inspection
- Product testing
- Development of private, national and international standards
- Management systems training
- Information on standards and international trade

Part 1 of the British Standard 7799, which defines a code of practice for information security management, has also been adopted as an International Standard ISO 17799 by the International Organisation for Standardisation. Part 2 is known as BS 7799-2:2002 “Specification for information security management” and is used to audit conformance with the BS7799/ISO17799. BS7799/ISO17799 is increasingly used worldwide, and in response the BSI offers two training and qualification programs for BS7799 auditors:

- BS 7799 Internal Auditor
- BS 7799 Lead Auditor

British Standard 7799 Lead Auditor

The BSI offers a five day intensive course to prepare candidates for the BS 7799 Lead Auditor examination. The course covers the following topics:

- BS 7799:1999
- Information security
- The importance of information security
- Assessing security threats and vulnerabilities
- Management of security risks
- Selecting security controls
- How to build an Information Security Management System (ISMS)
- Auditing to BS 7799
- BS 7799 auditing techniques
- Managing and leading a BS 7799 audit team
- Interview techniques
- Audit reporting

The course and the qualification is appropriate for the following individuals:

- Those wishing to implement a formal Information Security Management System (ISMS) in accordance with BS 7799 Part 2
- Existing security auditors who wish to expand their auditing skills
- Consultants who wish to provide advice on BS 7799 systems certification
- IT and Quality Control/Assessment Professionals

For more information on the course, examination and the qualification please contact the BSI.

British Standard 7799 Internal Auditor

This two-day course is aimed at internal auditors and managers interested in BS 7799 for use within their organisations. The course covers the following topics:

- Structure and definitions in ISO 19011
- Security system requirements
- Planning an audit
- Producing checklists
- Performing a security audit
- Reporting the audit findings
- Implementing corrective actions
- Follow-up options
- Continual improvement

After attending the course the participants will have an understanding of the following subjects:

- The key requirements of BS 7799-2:2002
- Auditing best practice as defined by ISO 19011:2002
- How to plan, execute and report a security audit
- The importance of information security and compliance
- How the audit process facilitates the continual improvement of security controls
- The benefits of implementing corrective and preventive actions.

For more information on BS 7799 Internal Auditor course please contact the BSI.

British Computer Society

Website:	www.bcs.org.uk
E-mail:	bcshq@hq.bcs.org.uk
Address:	1 Sanford Street Swindon, Wiltshire SN1 1HJ United Kingdom
Phone:	+44 1793 417417
Fax:	+44 1793 480270

The British Computer Society is the United Kingdom's only chartered professional institution for Information Technology founded in 1957 and granted a Royal Charter in 1984. The British Computer Society is also an engineering institution, fully licensed by the UK Engineering Council to nominate Chartered and Incorporated Engineers and to accredit university courses and training schemes, and represents the United Kingdom at the International Federation for Information Processing (IFIP).

BCS offers several professional qualifications in information technology, and one of them is the Certificate in Information Security Management Principles.

Certificate in Information Security Management Principles

The Certificate in Information Security Management Principles is a foundation-level qualification in information security management for those who are new to the field or who would like to formalise their existing knowledge. Two qualification routes exist: the training route and the experienced route. Training route candidates must attend an accredited training course and have a minimum one year's IT work experience; whereas the experienced route candidates must have one year's IT work experience with at least six months experience in one or more of the ten areas defined by the British Standard 7799, Code of Practice for Information Security Management. The following subject areas are covered by the Certificate:

- Concepts & definitions
- The need for, and benefits of, information security
- Threats to information systems
- Managing information security
- Information security risk analysis
- Legal framework
- Security standards and procedures
- Principles of conduct
- Safeguards
- Business continuity
- Implementation

The Certificate examinations are held regularly at British Computer Society offices in London; for information on examination dates and fees please visit the BCS at www.bcs.org.uk.

ASIS International

Website:	www.asisonline.org
E-mail:	asis@asisonline.org
Address:	1625 Prince Street Alexandria, VA 22314-2818, USA
Phone:	+1 703 519 6200
Fax:	+1 703 519 6299

ASIS International, previously known as the American Society for Industrial Security, was founded in 1955 and has more than 33,000 members and 208 chapters worldwide. ASIS is the world's leading organisation of security management and physical security professionals. In addition to professional conferences, seminars and exhibitions ASIS also maintains a respected professional certification program. Since information security also includes physical security, ASIS and its qualifications are included in this handbook. ASIS International offers three qualifications in security which are introduced on the following pages:

- Certified Protection Professional (CPP)
- Physical Security Professional (PSP)
- Professional Certified Investigator (PCI)

Certified Protection Professional (CPP)

CPP is one of the most respected and recognised qualifications in security management and physical security. Before being allowed to take the CPP examination CPP candidates have to satisfy the following requirements: have at least nine (9) years of full-time security experience with at least three (3) years in a position responsible for security or hold a recognised Bachelor's degree and have seven (7) years of experience. Provided the candidates meet experience criteria have no criminal convictions they can register for and take the CPP 200 multiple-choice questions examination which covers the following seven domains:

1. Security management	38%
2.Investigations	15%
3.Legal aspects	7%
4. Personnel security	9%
5.Physical security	19%
6.Protection of sensitive information	6%
7. Emergency management	6%

Certified Protection Professionals must adhere to ASIS's Professional Responsibility Code as a condition of certification. ASIS examination fees range from US$ 200 to US$ 350 depending on the examination location and ASIS membership status. For more information on the CPP designation, location of examination centres and CPP exam preparation resources please visit ASIS International online at www.asisonline.org.

Physical Security Professional (PSP)

Those professionals who specialise or wish to specialise in physical security should consider ASIS International's Physical Security Professional qualification. Requirements for PSP certification include the following:

- Five (5) years of experience in the physical security field
- High school diploma or general education equivalent
- The applicant must not have been convicted of any criminal offence that would reflect negatively on the security profession, ASIS, or the certification program

The PSP examination covers the following three domains in a multiple-choice questions format:

1. Physical security assessment	41%
2.Selection of integrated physical security measures	24%
3.Implementation of physical security measures	35%

The PSP examination fees range from US$ 300 to US$ 350 depending on the location of the examination centre and candidate's ASIS membership status. Like with other ASIS qualifications, Physical Security Professionals must adhere to the ASIS Professional Responsibility Code. For up to date information on the PSP certification program please visit ASIS International website at www.asisonline.org.

Professional Certified Investigator (PCI)

The Professional Certified Investigator qualification from the ASIS International is targeted at security professionals who specialise in investigation – case management, evidence collection, and case presentation. The PCI examination therefore covers the following three domains using a multiple-choice questions format:

1. Case management	40%
2.Evidence collection	40%
3.Case presentation	20%

Before being allowed to take the PCI examination the candidates must satisfy the following pre-qualification requirements:

- Nine (9) years of investigations experience, with at least three (3) years in case management; or
- An earned Bachelor's degree or higher from an accredited institution of higher education and seven (7) years of investigations experience, at least three (3) years of which shall have been in case management
- The applicant must not have been convicted of any criminal offence that would reflect negatively on the security profession, ASIS, or the certification program.

ASIS Professional Responsibility Code requirements apply. The PCI examination fees range from US$ 300 to US$ 350 depending on the ASIS membership status of candidates. For more information regarding the PCI qualification please visit ASIS at www.asisonline.org.

DRI International

Website:	www.drii.org
E-mail:	driinfo@drii.org
Address:	201 Park Washington Court Falls Church, VA 22046-4513, USA
Phone:	+1 703 538 1792
Fax:	+1 703 241 5603

Founded in 1988 as the Disaster Recovery Institute, DRI International's goals are to promote business continuity planning and disaster recovery through education, assistance, and publication of standards; certify qualified individuals in the discipline; and promote the credibility and professionalism of certified individuals. DRI International currently offers three levels of certification:

- Associate Business Continuity Planner (ABCP)
- Certified Business Continuity Professional (CBCP)
- Master Business Continuity Professional (MBCP)

Associate Business Continuity Planner (ABCP)

The Associate Business Continuity Planner certification is the first of the three professional qualifications awarded by Disaster Recovery Institute International. It is an entry-level qualification intended for those candidates who have less than two years of business continuity or disaster recovery planning or who otherwise don't qualify for the Certified Business Continuity Professional designation. To earn the Associate Business Continuity Planner qualification candidates must first receive a passing score on the DRII examination (75%) and then apply for certification. The examination covers the following ten subject areas of the Professional Practices for the Business Continuity Planners:

- Project initiation and management
- Risk evaluation and control
- Business impact analysis
- Developing business continuity strategies
- Emergency response and operations
- Developing and implementing business continuity plans
- Awareness and training programs
- Maintaining and exercising business continuity plans
- Public relations and crisis coordination
- Coordination with public authorities

DRII offers training courses and publications in addition to certification. The DRII examination fee is US$ 250. An application fee of US$ 50 is also applicable. Please visit DRII online at www.drii.org for more information.

Certified Business Continuity Professional (CBCP)

Certified Business Continuity Professional is the core qualification awarded by the DRI International to those candidates who

- Have at least two years of business continuity and/or disaster recovery planning work experience
- Receive a passing score (75%) on the DRII examination
- Provide at least two suitable professional references

The DRII examination tests the candidates on the ten subject areas of the Professional Practices for the Business Continuity Planners:

- Project initiation and management
- Risk evaluation and control
- Business impact analysis
- Developing business continuity strategies
- Emergency response and operations
- Developing and implementing business continuity plans
- Awareness and training programs
- Maintaining and exercising business continuity plans
- Public relations and crisis coordination
- Coordination with public authorities

DRII application fee for CBCP candidates is US$ 250 in addition to the DRII examination fee of US$ 250. Continuing professional education requirements also apply to Certified Business Continuity Professionals.

For up to date information on the CBCP designation please visit DRII online at www.drii.org.

Master Business Continuity Professional (MBCP)

For those candidates who have demonstrated significant knowledge and experience in the business continuity and/or disaster recovery planning DRII offers the Master Business Continuity Professional (MBCP) designation. MBCP requirements include the following:

- At least five years of business continuity and/or disaster recovery planning work experience
- Score of 85% or higher on the DRII examination
- Completion of a case study exam or a Masters-thesis level directed research project
- Provision at least two suitable professional references

Like ABCP and CBCP candidates, MBCP candidates are tested on the ten subject areas of the Professional Practices for the Business Continuity Planners:

- Project initiation and management
- Risk evaluation and control
- Business impact analysis
- Developing business continuity strategies
- Emergency response and operations
- Developing and implementing business continuity plans
- Awareness and training programs
- Maintaining and exercising business continuity plans
- Public relations and crisis coordination
- Coordination with public authorities

In addition to the DRII examination fee of US$ 250, MBCP candidates also have to pay an application fee of US$ 300.

For a complete description of MBCP requirements and up to date information please visit www.drii.org.

Association of Certified Fraud Examiners

Website:	www.cfenet.com
E-mail:	info@cfenet.com
Address:	716 West Avenue Austin, TX 78701-2727, USA
Phone:	+1 512 478 9000
Fax:	+1 512 478 9297

Association of Certified Fraud Examiners is an international professional organisation founded in 1988 in Austin, Texas. With more than 28,000 members in more than 100 countries worldwide ACFE is dedicated to fighting fraud in its many forms. ACFE members and Certified Fraud Examiners include, inter alia, auditors, accountants, fraud investigators, loss prevention specialists, attorneys, educators, and criminologists. In addition to its certification program, the Association also provides training and networking opportunities.

Certified Fraud Examiner (CFE)

Certified Fraud Examiners are qualified professionals who specialise in fraud prevention and detection. To achieve the Certified Fraud Examiner designation candidates must satisfy the following requirements:

- Be of high moral character
- Meet minimum academic and professional requirements
- Successfully complete the Uniform CFE Examination (mandatory for US, Canada and UK residents)
- Maintain required continuing professional education
- Be an Associate Member of ACFE in good standing (required for US, Canada and UK residents)
- Agree to abide by the Bylaws and Code of Professional Ethics of the Association of Certified Fraud Examiners
- Pay annual ACFE dues

The uniform CFE examination is computer-based and consists of 500 objective and true/false questions covering the following four subjects (125 questions each):

- Financial transactions
- Legal elements of fraud
- Fraud investigation
- Criminology and ethics

CFE preparation materials are available from the Association. The uniform CFE examination fee is US$ 200. Certified Fraud Examiners are required to satisfy continuing professional education requirements and pay annual fees in order to keep their certification valid. For more detailed information on the CFE designation and certification requirements please visit the Association of Certified Fraud Examiners online at www.cfenet.com.

CERT Coordination Center

Website:	www.cert.org
E-mail:	training-info@cert.org
Address:	CERT Coordination Center Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213-3890, USA
Phone:	+1 412 268 7090
Fax:	+1 412 268 6989

One of the best known and most respected information security organisations the CERT Coordination Center also provides training and certification programme for computer security incident handling specialists – the CERT Certified Computer Security Incident Handler qualification.

CERT Certified Computer Security Incident Handler

The CERT Certified Computer Security Incident Handler certification is targeted at information security practitioners with three or more years of work experience in incident handling with certification requirements as follows:

a) Completion of four courses:
- Creating a Computer Security Incident Response Team (1 day)
- Information security for technical staff (5 days)
- Managing Computer Security Incident Response Teams (3 days) or Fundamentals of incident handling (5 days)
- Advanced incident handling (5 days)

b) One elective course from the following topics. Course must be taken from an ABET-accredited college or university or must be the equivalent of 5 continuing education units (CEUs):
- computer forensics
- intrusion detection and analysis
- security audits and assessments

c) Three years of experience in the incident handling;
d) Letter of recommendation from current or previous manager; and
e) Successful completion of an evaluation administered by the Software Engineering Institute.
f) Recertification is required every three years.

For detailed and up to date information on this certification and its requirements please visit the CERT Coordination Center at www.cert.org.

High Tech Crime Network

Website:	www.htcn.org
E-mail:	info@htcn.org
Phone:	+1 973 726 9328

The High Tech Crime Network formed in 1991 is a network of law enforcement agencies and corporate security professionals from fifteen countries including United States, United Kingdom, Belgium, Canada, Germany, Norway, and others. In operation for more than ten years the High Tech Crime Network trains and certifies high tech crime specialists. Currently four certifications are offered:

- Certified Computer Crime Prosecutor
- Certified Computer Crime Attorney
- Certified Computer Crime Investigator
- Certified Computer Forensics Technician

Certified Computer Crime Prosecutor

Candidates for the Certified Computer Crime Prosecutor qualification are required to meet the following requirements:

- Two years prosecutorial experience in any discipline
- Two years prosecutorial experience directly related to computer crimes investigation
- Successfully complete eighty hours of computer crimes training via on-site course(s) provided by an approved organisation
- Successfully demonstrate their technical knowledge by completing a written exam

For detailed and up to date information on this qualification please contact the High Tech Crime Network at info@htcn.org.

Certified Computer Crime Attorney

The requirements for the Certified Computer Crime Attorney certification are as follows:

- Two years experience as an attorney in any discipline
- Two years experience as an attorney directly related to computer crimes investigation
- Successful completion of eighty hours of computer crimes training via on-site course(s) provided by an approved organisation
- Successful completion of a written exam

For detailed and up to date information on this qualification please contact the High Tech Crime Network at info@htcn.org.

Certified Computer Crime Investigator

Certified Computer Crime Investigator candidates must meet the following certification requirements:

- Two years investigative experience in any discipline or a college degree and one year investigative experience in any discipline
- Two years investigative experience directly related to computer crimes investigation
- Successful completion of eighty hours of computer crimes training via on-site course(s) provided by an approved organisation
- Successful completion of a written exam

For detailed and up to date information on this qualification please contact the High Tech Crime Network at info@htcn.org.

Certified Computer Forensics Technician

Certified Computer Forensics Technician candidates must meet the following certification requirements before being awarded this designation:

- Two years investigative experience in any discipline or a college degree and one year investigative experience in any discipline
- Two years investigative and hands-on experience directly related to computer forensics
- Successful completion of eighty hours of computer forensics training via on-site course(s) provided by an approved organisation
- Successful completion of a written exam

For detailed and up to date information on this qualification please contact the High Tech Crime Network at info@htcn.org.

International Information Systems Forensics Association

Website:	www.infoforensics.org
Address:	300 Satellite Blvd Suwanee, GA 30024, USA

The International Information Systems Forensics Association is the professional organisation of the information forensics community. Members of the Association come from different backgrounds – such as law enforcement, information security, management, and others – and are dedicated to the advancement of information forensics. The Association also administers a professional certification scheme for information forensics specialists – the Certified Information Forensics Investigator (CIFI) designation.

Certified Information Forensics Investigator (CIFI)

Certified Information Forensics Investigator candidates must successfully complete the 200 multiple choice questions long CIFI examination which covers the following six domains:

- Auditing
- Incident response
- Law and investigation
- Tools and techniques
- Traceback
- Countermeasures

The CIFI examination fee is US$ 450; recommended reading list for exam preparation is available from the Association. Association training partners also provide training for the CIFI designation. For more detailed and up to date information on this qualification please visit the International Information Systems Forensics Association at www.infoforensics.org.

International Association of Computer Crime Investigative Specialists

Website:	www.cops.org
E-mail:	iadmin@cops.org
Address:	P.O. Box 140, Donahue, IA 52746-0140, USA
Phone:	+1 563 326 6118

The International Association of Computer Crime Investigative Specialists (IACIS) is a volunteer non-profit organisation of law enforcement professionals dedicated to education in and development of the computer forensics as a science. The Association also administers the Certified Forensic Computer Examiner (CFCE) certification.

Certified Forensic Computer Examiner (CFCE)

The Certified Forensic Computer Examiner qualification is granted in two ways: through the training route, by attending a two-week long course administered by the Association, or through examination, by successfully passing a rigorous practical computer forensics examination which is intended to demonstrate computer forensics skills and knowledge in practice. Candidates who are certified are required to meet continuing professional education requirements set by the Association.

The certification fee for those candidates who choose to apply for certification through examination route is US$ 750 and they have up to five months to complete the examination requirements.

For detailed and up to date information on CFCE training and examination schemes please visit IACIS at www.cops.org.

Part II

Vendor Qualifications

Cisco Systems

Website:	www.cisco.com
Address:	170 West Tasman Drive San Jose, CA 95134, USA
Phone:	+1 408 526 4000

Cisco Systems is one of the world's leading networking and security solutions vendors. In addition to its comprehensive internetworking products line Cisco is also a leading provider of integrated solutions, consulting, training, and certification. Currently the following security certifications are available from Cisco Systems:

- Cisco Certified Internetwork Expert Security
- Information Systems Security Professional
- Cisco Certified Security Professional
- Cisco Firewall Specialist
- Cisco Intrusion Detection System Specialist
- Cisco Virtual Private Networks Specialist

Cisco Certified Internetwork Expert Security (CCIE Security)

CCIE Security is Cisco Systems' highest security certification intended to identify top network security experts. Introduced after the international success of the Cisco Certified Internetwork Expert in Routing and Switching certification, CCIE Security continues Cisco's tradition of certification excellence in the network security area. Although CCIE Security is a vendor qualification and largely focuses on Cisco Systems' solutions it also requires a deep understanding of network security and protocols as a whole.

CCIE Security certification requirements consist of the following:

- A passing score on the 100 questions long multiple choice computerised CCIE Security qualification exam administered at VUE and Prometric testing centres worldwide; and
- A passing score on the practical one-day laboratory exam administered at a Cisco CCIE testing laboratory.

The first examination is intended to test candidate's theoretical knowledge of network security and Cisco solutions; the second practical lab exam tests candidates on their ability to apply theoretical knowledge in solving practical problems and implementing Cisco security solutions. Candidates must first obtain a passing score on the qualification exam before being allowed to register for and take the practical lab exam.

The cost of both CCIE Security examinations is US$ 1,550 (US$ 300 + 1,250) not including training, preparation materials or travel.

For more information on the CCIE Security certification and up to date certification requirements please visit Cisco Systems at www.cisco.com.

Information Systems Security Professional (INFOSEC)

By virtue of a certification granted to Cisco Systems by the U.S. National Security Agency and the U.S. Committee on National Security Systems (CNSS) those who satisfy the following requirements (completion of 5 exams) are recognised as Information Systems Security Professionals under the NSA 4011 training standard:

- Cisco Certified Network Associate (CCNA)
- Securing Cisco IOS Networks (Exam 642-501)
- Cisco Secure PIX Firewall Advanced (Exam 642-521)
- Cisco Secure Virtual Private Networks (Exam 642-511)
- Cisco Secure Intrusion Detection Systems (643-531)

For more information on the Information Systems Security Professional (INFOSEC) certification please visit Cisco Systems at www.cisco.com and the U.S. National Security Agency at www.nsa.gov.

Cisco Certified Security Professional (CCSP)

The Cisco Certified Security Professional certification is a relatively recent addition to the existing Cisco Professional qualifications (Cisco Certified Network, Design and Internet Professional – CCNP, CCDP, CCIP). CCSP is a professional qualification in its own right; however, it may also be seen as a stepping stone to the Cisco Certified Internetwork Expert in Security. To obtain the CCSP designation candidates must satisfy the following requirements:

a) Hold a valid CCNA or CCIP certification
b) Pass the following exams:
   - Securing Cisco IOS Networks (Exam 642-501)
   - Cisco Secure PIX Firewall Advanced (Exam 642-521)
   - Cisco Secure Intrusion Detection System (Exam 643-531)
   - Cisco Secure VPN (Exam 642-511)
   - Cisco SAFE Implementation (Exam 642-541)

The CCSP designation is valid for three years and must be renewed by passing the current versions of appropriate examinations. For more information on available training and resources please visit Cisco Systems at www.cisco.com.

Cisco Firewall Specialist

The Cisco Firewall Specialist qualification demonstrates understanding and knowledge of Cisco firewall solutions – Cisco IOS and Cisco Private Internet Exchange (PIX). The requirements for the Cisco Firewall Specialist designation are as follows:

a) Valid CCNA certification and
b) passing score on the following 2 examinations:
- Securing Cisco IOS Networks (Exam 642-501)
- Cisco Secure PIX Firewall Advanced (Exam 642-521)

The Cisco Firewall Specialist certification is valid for two years and must be renewed by passing current versions of appropriate examinations. For more information please visit www.cisco.com.

Cisco Intrusion Detection System Specialist

The Cisco IDS Specialist certification is one of the three Cisco security specialist qualifications. Cisco IDS Specialists are examined on their mastery of Cisco IOS and Cisco Secure Intrusion Detection System solutions. The requirements for the Cisco IDS Specialist certification are as follows:

a) Valid CCNA certification and
b) passing scores on the following 2 examinations:

- Securing Cisco IOS Networks (Exam 642-501)
- Cisco Secure Intrusion Detection System (Exam 643-531)

Like other Cisco specialist certifications the Cisco IDS Specialist qualification is valid for two years and must be renewed by passing the current versions of appropriate examinations.

Cisco Virtual Private Networks Specialist

Like the other two Cisco security specialist designations (Cisco Firewall Specialist and Cisco IDS Specialist) the Cisco VPN Specialist qualification requires a valid Cisco Certified Network Associate (CCNA) certification and passing grades on the following two examinations:

- Securing Cisco IOS Networks (Exam 642-501)
- Cisco Secure Virtual Private Networks (Exam 642-511)

Cisco VPN Specialist certification is valid for two years and must be renewed by passing the current versions of appropriate examinations. For information on training and exam registration please visit Cisco Systems at www.cisco.com.

Check Point Software Technologies

Website:	www.checkpoint.com
E-mail:	info@checkpoint.com
Address:	3A Jabotinsky St., Diamond Tower Ramat Gan 52520, Israel
Phone:	+972 3 753 4555
Fax:	+972 3 575 9256

Founded in 1993 and with headquarters in Israel and the United States Check Point Software Technologies is one of the leading network security solutions providers. Check Point is particularly well known for their firewall and virtual private network (VPN) solutions. To complement their solution offerings Check Point also administers a certification program which includes the following qualifications:

- Check Point Certified Security Principles Associate (CCSPA)
- Check Point Certified Security Administrator (CCSA)
- Check Point Certified Security Expert (CCSE)
- Check Point Certified Security Expert Plus (CCSE Plus)
- Check Point Certified Managed Security Expert (CCMSE)

In addition to certification Check Point also offers training programs intended to prepare candidates for these certification examinations – for details of these programs please visit Check Point at www.checkpoint.com.

Check Point Certified Security Principles Associate (CCSPA)

The CCSPA is Check Point's entry-level certification which is intended to demonstrate candidate's knowledge of security fundamentals, concepts and best practices.

The CCSPA certification also places particular emphasis on the understanding of relationship between business needs and network security solutions.

To earn the CCSPA designation candidates must take and pass the CCSPA exam 156-110 at a VUE testing centre.

For more information on CCSPA exam objectives and training resources please visit Check Point at www.checkpoint.com.

Check Point Certified Security Administrator (CCSA)

The Check Point Certified Security Administrator designation is for those candidates who configure and manage Check Point FireWall-1 firewalls.

The CCSA is a foundation-level qualification and requires a passing score on the *Check Point NG with Application Intelligence – Management I* exam 156-210.4 which may be taken at VUE testing centres.

For more information on the Check Point Certified Security Administrator qualification please visit www.checkpoint.com.

Check Point Certified Security Expert (CCSE)

The Check Point Certified Security Expert designation is the next step after the Check Point Certified Security Administrator qualification for those who would like to acquire certification of their Check Point VPN-1 skills in addition to FireWall-1. To earn the CCSE designation candidates must take and pass the following examinations:

- Check Point NG with Application Intelligence – Management I (Exam 156-210.4)
- Check Point NG with Application Intelligence – Management II (Exam 156-310.4)

CCSE candidates who already hold the CCSA designation need only to sit and pass exam 156-310.4 to achieve the CCSE status.

Check Point Certified Security Expert Plus (CCSE Plus)

CCSE Plus is an advanced certification built on top of the CCSA and CCSE qualifications which shows in-depth understanding of Check Point VPN-1 and FireWall-1 solutions. CCSE Plus holders also have demonstrated knowledge in network planning, implementation and troubleshooting. To be awarded the CCSE Plus designation candidates must pass the following examinations:

- Check Point NG with Application Intelligence – Management I (Exam 156-210.4)
- Check Point NG with Application Intelligence – Management II (Exam 156-310.4)
- Check Point NG with Application Intelligence – Management III (Exam 156-510.4)

Therefore CCSA and CCSE holders have to take and pass exam 156-510.4 only to achieve the CCSE Plus designation.

Check Point Certified Managed Security Expert (CCMSE)

The CCMSE designation is an advanced management qualification which requires CCSA and CCSE certifications as prerequisites.

CCMSE certifies holders' both technical and management expertise in planning, implementing and managing VPN-1, FireWall-1 and Provider-1 Check Point security solutions.

To achieve the CCMSE designation candidates must pass the following examinations:

- Check Point NG with Application Intelligence – Management I (Exam 156-210.4)
- Check Point NG with Application Intelligence – Management II (Exam 156-310.4)
- Managing Multiple Sites Using Provider-1 NG (Exam 156-810)

For exam objectives please visit www.checkpoint.com.

Check Point Certified Managed Security Expert Plus VSX (CCMSE Plus VSX)

Check Point VPN-1/FireWall-1 VSX is a high-speed multi-policy security solution designed for Virtual Local Area Networks (VLANs).

The CCMSE Plus VSX designation is awarded to those CCMSE holders who have also passed the VPN-1/FireWall-1 VSX Management exam 156-811 and therefore requires CCSA, CCSE, and CCMSE certifications as prerequisites.

For more information about the VSX solution and the CCMSE Plus VSX certification please visit Check Point at www.checkpoint.com.

Internet Security Systems

Website:	www.iss.net
Address:	6303 Barfield Road Atlanta, GA 30328, USA
Phone:	+1 404 236 2600

Founded in 1994 Internet Security Systems operates in 27 countries around the world. Backed by a professional research & development team ("ISS X-Force") Internet Security Systems offer Internet security products and services, including the BlackICE firewall family and managed network security solutions.

Three certifications are offered by Internet Security Systems to those specialists who have demonstrated mastery of ISS solutions at progressive levels:

- ISS Certified Specialist
- ISS Certified Expert
- ISS Certified Architect

ISS Certified Specialist (ISS-CS)

The ISS Certified Specialist certification is the entry-level ISS qualification. To be awarded the ISS Certified Specialist certification candidates must satisfy the following requirements:

- Have an understanding of ISS RealSecure solutions
- Have minimum of three months practical experience with ISS RealSecure solutions
- Have understanding of network and security principles
- Pass two examinations from either of two offered certification tracks

Currently there are two ISS-CS certification tracks:

Track 1
- Introduction to RealSecure
- Internet Scanner

Track 2
- Introduction to RealSecure SiteProtector
- Internet Scanner

ISS examinations are held around the world at VUE testing centres. For more information on training and requirements for this certification please visit www.iss.net.

ISS Certified Expert (ISS-CE)

The ISS Certified Expert certification is the practitioner-level ISS qualification for professionals already holding the ISS Certified Specialist qualification. To obtain certification as an ISS Certified Expert the candidates must satisfy the following requirements:

- Hold ISS Certified Specialist certification
- Have advanced knowledge of ISS RealSecure solutions
- Have at least six months of practical experience with ISS RealSecure solutions
- Have intermediate understanding of TCP/IP networking
- Have intermediate understanding of Windows and UNIX operating systems
- Have basic understanding of security principles
- Pass one exam from either of two certification tracks

The two certification tracks available for ISS Certified Expert candidates are as follows:

- Track 1 – Advanced RealSecure
- Track 2 – Advanced SiteProtector

For more information on recommended training and costs involved please visit ISS online at www.iss.net.

ISS Certified Architect (ISS-CA)

ISS Certified Architect is the highest qualification awarded by Internet Security Systems. It is reserved for professionals who already hold the ISS Certified Expert designation and are able to demonstrate deep understanding of not only ISS solutions but also professional-level knowledge of TCP/IP, vulnerability assessment, Windows, UNIX, intrusion detection, and various attack methods. To achieve the ISS Certified Architect certification candidates must satisfy the following requirements:

- Hold the ISS Certified Expert designation
- Have 9–12 months of network security work experience
- Have deep understanding of TCP/IP, Windows and UNIX
- Have knowledge of vulnerability assessment and intrusion detection tools
- Be familiar with various attack methods
- Have network traffic and log analysis experience
- Pass one exam from either of two ISS-CA certification tracks

The two ISS-CA certification tracks are

- Track 1 – Network intrusion and penetration techniques
- Track 2 – Advanced intrusion detection

For more information on training and preparation for ISS-CA please visit Internet Security Systems at www.iss.net. ISS examinations are conducted at authorised VUE testing centres.

Sun Microsystems

Website:	suned.sun.com
Address:	4150 Network Circle Santa Clara, CA 95054, USA
Phone:	+1 650 960 1300

Sun Microsystems, founded in 1982, is one of the leading enterprise client/server solution providers. Sun Microsystems' SPARC systems and Solaris operating environment are used for their reliability, standards conformance and open architecture. Sun Microsystems is also a first class centre of research and development – Java was born at Sun. Sun Microsystems has a developed certification programme which includes the Sun Certified Security Administrator qualification.

Sun Certified Security Administrator

The Sun Certified Security Administrator certification is for Solaris system administrators who have at least six months of work experience with the Solaris operating environment. Although Sun Certified Security Administrator candidates are not required to hold Sun Certified System or Network Administrator certifications, these certifications are recommended before attempting the Sun Certified Security Administrator examination.

The Sun Certified Security Administrator examination is available at Prometric testing centres and is a multiple-choice questions test consisting of 60 questions to be answered in 90 minutes. The examination covers the following subjects:

- General security concepts
- Detection and device management
- Security attacks
- File and system resources protection
- Host and network protection
- Network connection access, authentication and encryption

Training and study guides for the Sun Certified Security Administrator certification is available from both Sun Microsystems and third parties. For more information please visit Sun Microsystems at www.sun.com.

Microsoft Corporation

Website:	www.microsoft.com
E-mail:	mcphelp@microsoft.com
Address:	One Microsoft Way Redmond, WA 98052-6399, USA

Microsoft Corporation offers two Microsoft Windows security related certifications:

- Microsoft Certified Systems Administrator: Security
- Microsoft Certified Systems Engineer: Security

Microsoft Certified Systems Administrator: Security (MCSA Security)

The requirements for the MCSA certification with specialisation in security are passing scores on the following three core and two security specialisation examinations:

- Installing, configuring and administering Windows 2000 Pro (Exam 70-210) or
- Installing, configuring and administering Windows XP Pro (Exam 70-270)
- Installing, configuring and administering Windows 2000 Server (Exam 70-215)
- Managing a Windows 2000 network environment (Exam 70-218)
- Implementing and administering security in a Windows 2000 network (Exam 70-214)
- Installing, configuring and administering ISA Server 2000 Enterprise (Exam 70-227) or
- CompTIA Security+ (Exam SY0-101)

Training for the MCSA Security is available from Microsoft and includes both instructor-led courses and self-study books. Additionally a worldwide network of Microsoft training partners provides training for Microsoft certifications. For up to date information on MCSA Security please visit Microsoft at www.microsoft.com.

Microsoft Certified Systems Engineer: Security (MCSE Security)

As a more advanced certification than MCSA Security, the Microsoft Certified Systems Engineer: Security requirements include passing scores on four core and three security specialisation examinations:

- Installing, configuring and administering Windows 2000 Pro (Exam 70-210) or
- Installing, configuring and administering Windows XP Pro (Exam 70-270)
- Installing, configuring and administering Windows 2000 Server (Exam 70-215)
- Implementing and administering a Windows 2000 network infrastructure (Exam 70-216)
- Implementing and administering a Windows 2000 Directory Services Infrastructure (Exam 70-217)
- Designing security for a Windows 2000 network (Exam 70-220)
- Implementing and administering security in a Windows 2000 network (Exam 70-214)
- Installing, configuring and administering ISA Server 2000 Enterprise (Exam 70-227) or
- CompTIA Security+ (Exam SY0-101)

Training for MCSE Security is available from Microsoft and includes both instructor-led courses and self-study books. Additionally a worldwide network of Microsoft training partners provides training for Microsoft certifications. For up to date information on MCSE Security please visit Microsoft at www.microsoft.com.

Bindview Corporation

Website:	www.bindview.com
E-mail:	psquestions@bindview.com
Address:	5151 San Felipe, Suite 2500 Houston, TX 77056, USA
Phone:	+1 713 561 4000
Fax:	+1 713 561 1000

Bindview Corporation is a provider of proactive business policy compliance, vulnerability management, and directory administration and migration solutions. As part of their solutions they offer a training and certification programme leading to the Bindview Certified Security Professional (BCSP) designation.

Bindview Certified Security Professional (BCSP)

The Bindview Certified Security Professional certification is intended for security auditors who use and implement Bindview solutions in Microsoft Windows environments. The prerequisites for this qualification are familiarity with Microsoft Windows and Exchange environments as well as general knowledge of information security concepts. Previous information security experience is recommended. Bindview offers a five days long BCSP training course which prepares students to take and pass the BCSP examination. The following topics are covered in the course and the exam:

- Ten domains of computer security
- Security standards and best practices
- The role of policy and procedures
- The bv-Control product suite
- Vulnerability assessment

For more information on Bindview solutions and the Bindview Certified Security Professional certification please visit Bindview Corporation at www.bindview.com.

Enterasys Networks

Website:	www.enterasys.com
E-mail:	training@enterasys.com
Address:	50 Minuteman Road Andover, MA 01810, USA
Phone:	+1 603 337 0604
Fax:	+1 603 337 0610

Enterasys Networks provides enterprise network solutions for data centres, workgroups, and branch offices including intrusion detection, virtual private networks, switching, routing and network management solutions.

Among certifications offered by Enterasys Networks is the Enterasys Security Specialist / Enterasys Security Systems Engineer (ESS/ESSE) qualification.

Enterasys Security Specialist / Enterasys Security Systems Engineer (ESS/ESSE)

ESS/ESSE certified professionals have in-depth understanding and knowledge of Enterasys Networks' enterprise network security solutions, products and technologies. To achieve this certification candidates must sit and pass the following two examinations:

- ESS Policy Enabled Networking
- ESS Dragon Intrusion Detection System

Corresponding training courses for these two examinations are available from Enterasys Networks. Enterasys examinations may be taken at Prometric testing centres worldwide. The examination fees are US$ 199 per exam for exams administered in North America and US$ 100 for all other testing centres. For more information on Enterasys Networks certification programme please visit www.enterasys.com.

IBM/Tivoli

Website: www.ibm.com
E-mail: certify@us.ibm.com
Address: IBM/Tivoli Professional Certification
(101 2 E028)
11301 Burnet Road
Austin, TX 78758, USA

The IBM/Tivoli certification programme includes a number of certifications covering a wide range of IBM and Tivoli solutions. The following information security related vendor certifications are currently offered by IBM/Tivoli and introduced on the following pages:

- IBM Certified Advanced Deployment Professional: Tivoli Security Management Solutions 2003
- IBM Certified Deployment Professional: Tivoli Privacy Manager for e-business
- IBM Certified Deployment Professional: Tivoli Risk Manager
- Tivoli Certified Consultant: IBM Tivoli Access Manager for e-business
- Tivoli Certified Consultant: IBM Tivoli Access Manager for Business Integration
- Tivoli Certified Solutions Expert: IBM SecureWay Firewall for Windows NT
- Tivoli Certified Solutions Expert: IBM SecureWay Firewall for AIX

IBM Certified Advanced Deployment Professional

Tivoli Security Management Solutions 2003

To achieve the IBM Certified Advanced Deployment Professional: Tivoli Security Management Solutions 2003 candidates must pass five required examinations from the following list:

a) CompTIA Security+ (Exam SY0-101) and one of the following two exams:

- IBM Tivoli Access Manager for Business Integration Implementation (Exam 000-792)
- IBM Tivoli Access Manager for e-business Implementation (Exam 000-795)

b) And the following three examinations:

- IBM Tivoli Privacy Manager for e-business Implementation (Exam 000-788)
- IBM Tivoli Risk Manager Implementation (Exam 000-796)
- IBM Tivoli Identity Manager Implementation (Exam 000-797)

For more information on exam objectives and training available for this certification please visit IBM at www.ibm.com.

IBM Certified Deployment Professional

- Tivoli Privacy Manager for e-business
- Tivoli Identity Manager
- Tivoli Risk Manager

The IBM Certified Deployment Professional track includes in particular the three certifications listed above. The exam objectives for these three certifications are as follows:

Tivoli Identity Manager

- Performing basic installation of the prerequisite databases (DB2, Oracle or SQL), application servers (WebSphere or WebLogic) and LDAP directory servers (IBM Directory Server or SunOne Server)
- System administration skills including working knowledge of account management
- IBM Tivoli Identity Manager architecture and components
- Basic understanding of JavaScript, XML, DSML
- Working knowledge of LDAP
- Basic security concepts (encryption, SSL, HTTPS)
- General knowledge of shell scripting and TCP/IP
- Basic knowledge of TCP/IP

Tivoli Privacy Manager for e-business

- Understand ITPM architecture and components
- Plan an ITPM implementation
- Plan a monitor development project
- Perform basic prerequisite software configuration and verification
- Perform ITPM installation and configuration
- Perform policy deployment
- Perform monitor implementation
- Create and manage audit reports
- Tune ITPM for performance
- Troubleshoot installations and resolve problems

Tivoli Risk Manager

- Understand the IBM Tivoli Risk Manager architecture and components
- Design Risk Manager deployment architecture based on customer requirements/environment
- Perform basic installations of the prerequisite applications

- Install and configure Risk Manager server software and related components
- Install and configure Risk Manager sensors and adapters
- Maintain and configure Risk Manager rulebases
- Perform advanced Risk Manager administration tasks
- Instruct customer on how to differentiate incident events and take appropriate actions
- Perform maintenance and recovery tasks
- Generate reports
- Perform problem determination and troubleshooting

To achieve any of these three certifications candidates must pass a corresponding examination at a VUE or Prometric testing centre. For more information on these certifications, their exam objectives and available training please visit IBM at www.ibm.com.

Tivoli Certified Solutions Expert

- IBM SecureWay Firewall for Windows NT
- IBM SecureWay Firewall for AIX

The IBM SecureWay Firewall is available for both Windows NT and AIX operating systems, and accordingly two different examinations are offered. The following topics are covered in the examinations and are tested in a multiple-choice question examinations at Prometric and VUE testing centres:

- IBM SecureWay planning, installation and testing
- Application firewall requirements
- Secure network structure documentation
- Firewall response requirements
- Name resolution using DNS
- Configuring DNS
- Filtering rules
- IP routing through the firewall
- SOCKS server configuration
- Secure proxy accounts
- Secure account removal
- Secure e-mail service
- Firewall configuration validation
- Intrusion prevention and documentation

For more information on the IBM SecureWay Firewall and related certifications please visit IBM at www.ibm.com.

Tivoli Certified Consultant

Two Tivoli Certified Consultant certification specialisations exist: the IBM Tivoli Access Manager for e-business and IBM Tivoli Access Manager for Business Integration. The topics covered by these certification examinations are as follows:

IBM Tivoli Access Manager for e-business

- Planning
- Installation
- Configuration and customisation
- Programming
- Maintenance and troubleshooting

IBM Tivoli Access Manager for Business Integration

- Planning and evaluating current environment
- Installing and configuring
- Configuring logging and auditing
- Troubleshooting problems
- Performing administrative tasks

Each certification involves one multiple-choice questions examination which may be taken at VUE and Prometric testing centres. For a comprehensive introduction to the IBM Tivoli Access Manager suite and more detailed information on these certifications and corresponding training please visit IBM at www.ibm.com.

Netscreen Technologies

Website:	www.netscreen.com
E-mail:	info@netscreen.com
Address:	805 11th Avenue, Building 3 Sunnyvale, CA 94089, USA
Phone:	+1 408 543 2100

Netscreen Technologies provide a wide range of security products and solutions, including firewall, virtual private networking, denial of service protection, anti-virus, and intrusion prevention solutions. To complement these offerings and provide means to identify professionals with comprehensive mastery of Netscreen solutions the following certifications and appropriate training programs are also available:

- Netscreen Certified IDP Associate (NCIA)
- Netscreen Certified Security Associate (NCSA)
- Netscreen Certified Security Professional (NCSP)

Netscreen Certified IDP Associate (NCIA)

The Netscreen Certified IDP Associate certification is the entry-level qualification in the Netscreen certification programme. Appropriate for technical sales, support personnel and beginner network administrators the NCIA examination covers the following subjects:

- Identification of IDP components and architecture
- Understanding different modes of IDP implementation
- Installing the Sensor software, management server and UI
- Using the CLI to view and define system parameters
- Understanding different rulebases and attack signatures
- Creating policies using pre-defined templates
- IDP attack identification process
- Basic optimization, tuning and troubleshooting
- Defining custom services
- Identification of IDP usage and implementation
- Analyzing logs and generating reports
- Basic troubleshooting

The NCIA examination has 75 questions and is multiple-choice questions examination to be completed in 75 minutes. The passing score is 70%. For more information on the Netscreen Certified IDP Associate designation and available training programs please visit Netscreen Technologies at www.netscreen.com.

Netscreen Certified Security Associate (NCSA)

The NCSA is the base-level qualification of the Netscreen certification programme. This qualification enables holders to install, configure and administer Netscreen firewalls and security solutions. This designation demonstrates holders ability to

- Configure multi-level user administration
- Configure the IP environment to correctly support routes
- Configure the NetScreen firewall to permit and deny traffic
- Configure mapped and virtual IP addresses
- Configure VPN tunnels with manual keys and IKE
- Configure NetScreen and Remote Client for IKE VPN

The Netscreen Certified Security Associate examination is available at VUE training centres. For up to date information on available training and detailed exam objectives please visit Netscreen Technologies at www.netscreen.com.

Netscreen Certified Security Professional (NCSP)

This is the most advanced qualification in the Netscreen certification programme. Netscreen Certified Security Professionals have demonstrated mastery of Netscreen firewalls and security solutions and are able to:

- Design & configure VPN hub-and-spoke networks
- Configure NetScreen’s high availability solution
- Understanding policy based NAT
- Understand NetScreen’s troubleshooting commands
- Implement Layer 2 Tunnelling Protocol (L2TP) for VPNs
- Advanced troubleshooting of Policy, Routing, and IPsec VPNs including IKE
- Using PKI technologies for IPsec VPNs and device management
- Design and implement traffic management
- Secure management of NetScreen devices using SSH and SSL
- Syslog and SNMP configuration

To achieve the NCSP designation candidates must already hold the NCSA certification and pass two NCSP examinations which are available at VUE testing centres. For more information on Netscreen Technologies certifications and training please visit www.netscreen.com.

RSA Security

Website:	www.rsasecurity.com
Address:	174 Middlesex Turnpike Bedford, MA 01730, USA
Phone:	+1 781 515 5000
Fax:	+1 781 515 5010

RSA Security, founded by the inventors of the RSA public key cryptosystem (Rivest, Shamir and Adleman) is one of the most respected names in the information security industry. In addition to their products and solutions RSA Security also holds the annual RSA Conference, one of the most attended information security events, and sponsors cryptography research through RSA Laboratories, their research & development centre.

RSA Security maintains a professional certification programme for their RSA SecurID, ClearTrust and Keon product lines as outlined below:

Solution	**Available certifications**
RSA SecurID	*RSA Certified Systems Engineer* *RSA Certified Administrator* *RSA Certified Instructor*
RSA ClearTrust	*RSA Certified Systems Engineer*
RSA Keon Core PKI	*RSA Certified Systems Engineer*

RSA Certified Instructor (RSA/CI)

RSA SecurID

The RSA Certified Instructor certification is aimed at professionals who intend to teach RSA SecurID training courses. This is the highest RSA SecurID certification and requires RSA Certified Systems Engineer and RSA Certified Administrator designations as prerequisites. In addition RSA/CI candidates must also demonstrate their skills and knowledge at an instructor workshop and attend the courses they will be teaching.

RSA Certified Administrator (RSA/CA)

RSA SecurID

The RSA Certified Administrator (RSA/CA) qualification is for system and network administrators who administer and maintain RSA SecurID solutions in their enterprises. RSA Certified Administrators have the skills and knowledge to understand business and IT requirements, as well as implement and maintain RSA SecurID solutions. As a prerequisite RSA/CA candidates must have at least two years' work experience with TCP/IP, DNS, WWW, as well as Windows NT and UNIX operating systems.

To achieve the RSA Certified Administrator designation candidates must pass the RSA/CA examination at a VUE testing centre.

RSA Security offers a corresponding training course for the RSA/CA designation – RSA SecurID Administration.

For more detailed information about the RSA/CA certification please visit www.rsasecurity.com.

RSA Certified Systems Engineer (RSA/CSE)

RSA SecurID
RSA ClearTrust
RSA Keon Core PKI

The RSA Certified Systems Engineer (RSA/CSE) designation is available in all three RSA product lines – the RSA SecurID, ClearTrust and Keon Core PKI.

RSA SecurID Certified Systems Engineer

Candidates must have at least two years work experience with TCP/IP, remote access, WWW, network applications, network security, and Windows/UNIX operating systems. To achieve the RSA SecurID Certified Systems Engineer designation candidates must pass one examination at a VUE testing centre.

RSA ClearTrust Certified Systems Engineer

Candidates must have at least two years work experience with Windows NT or UNIX system administration, TCP/IP and DNS configuration and troubleshooting, WWW, LDAP, JDBC/ODBC, programming languages, and PKI fundamentals. To achieve this certification candidates must pass one examination at a VUE testing centre.

RSA Keon Core PKI Certified Systems Engineer

Candidates must have at least two years work experience with Windows NT or UNIX system administration, hardware installation, programming languages, TCP/IP, PKI fundamentals, IPSEC, virtual private networks, LDAP, and LDIF. To achieve this designation candidates must pass one examination at a VUE testing centre.

More information on training and preparation resources for these certifications, as well as comprehensive documentation on covered RSA solutions, are available from www.rsasecurity.com.

Sniffer Certification Program

Website:	www.networkassociates.com
E-mail:	sniffercertification@nai.com
Address:	Network Associates, Inc. 3965 Freedom Circle Santa Clara, CA 95054, USA

The Sniffer Certification Program is administered by Network Associates, Inc. after their acquisition of Sniffer Technologies. Sniffer certifications differentiate those network security professionals who have in-depth knowledge of Sniffer Technologies solutions. Currently three certifications are offered under the Sniffer Certification Program:

- Sniffer Certified Professional (SCP)
- Sniffer Certified Master (SCM)
- Sniffer Certified Expert (SCE)

Sniffer Certification Program examinations are available at Prometric testing centres. For more information on the full range of Sniffer solutions please visit Network Associates at www.networkassociates.com.

Sniffer Certified Professional (SCP)

Sniffer Certified Professionals are network engineers/administrators who have demonstrated mastery of Sniffer Technologies solutions. To earn the Sniffer Certified Professional designation candidates must pass one examination – *Troubleshooting with the Sniffer Portable Network Analyzer (Exam 1T6-101)* – at a Prometric testing centre. Training and preparation resources for the Sniffer Certified Professional certification is available from the Sniffer University, a training arm of Network Associates.

For more information on the SCP designation and corresponding training please visit Network Associates at www.networkassociates.com.

Sniffer Certified Master (SCM)

Sniffer Certified Experts who would like to advance their knowledge of network analysis and troubleshooting may progress to the Sniffer Certified Master (SCM) designation by passing any three of the following examinations:

- Sniffer distributed enterprise management (Exam 1T6-102)
- Troubleshooting and management with Sniffer Distributed (Exam 1T6-111)
- Sniffer distributed enterprise management (Exam 1T6-201)
- Ethernet network analysis & troubleshooting (Exam 1T6-202)
- WAN network analysis and troubleshooting (Exam 1T6-207)
- Sniffer portable switch expert analysis & troubleshooting (Exam 1T6-215)
- ATM network analysis & troubleshooting (Exam 1T6-218)
- Wireless LAN analysis & troubleshooting (Exam 1T6-222)
- TCP/IP network analysis & troubleshooting (Exam 1T6-303)
- Windows NT network analysis & troubleshooting (Exam 1T6-313)
- Windows 2000 network analysis & troubleshooting (Exam 1T6-323)

Training for these examinations is available from the Sniffer University at www.snifferu.com.

Sniffer Certified Expert (SCE)

Sniffer Certified Professionals who would like to advance their knowledge of network analysis and troubleshooting may progress to the Sniffer Certified Expert (SCE) designation by passing any two of the following examinations:

- Sniffer distributed enterprise management (Exam 1T6-102)
- Troubleshooting and management with Sniffer Distributed (Exam 1T6-111)
- Sniffer distributed enterprise management (Exam 1T6-201)
- Ethernet network analysis & troubleshooting (Exam 1T6-202)
- WAN network analysis and troubleshooting (Exam 1T6-207)
- Sniffer portable switch expert analysis & troubleshooting (Exam 1T6-215)
- ATM network analysis & troubleshooting (Exam 1T6-218)
- Wireless LAN analysis & troubleshooting (Exam 1T6-222)
- TCP/IP network analysis & troubleshooting (Exam 1T6-303)
- Windows NT network analysis & troubleshooting (Exam 1T6-313)
- Windows 2000 network analysis & troubleshooting (Exam 1T6-323)

Training for these examinations is available from the Sniffer University at www.snifferu.com.

Symantec

Website:	www.symantec.com
Address:	20330 Stevens Creek Blvd. Cupertino, CA 95014, USA
Phone:	+1 408 517 8000

Symantec Corporation is one of the leading providers of anti-virus and enterprise security solutions. The Symantec certification programme has four levels; all four levels require base knowledge of TCP/IP and at least one operating system. Candidates have two options for certification: they may either choose to take Symantec-only examinations towards their chosen qualification or take a mix of Symantec examinations together with one or more approved third-party vendor-neutral examinations:

Symantec Certified Security Engineer

- GIAC Firewall Analyst
- GIAC Incident Handler
- GIAC Intrusion Analyst
- GIAC Windows Security Administrator

Symantec Certified Technology Architect

- CompTIA Security+
- Certified Information Systems Security Professional
- Certified Protection Professional
- Certified Information Systems Auditor
- TruSecure ICSA Certified Security Associate
- CIW Security Analyst

Symantec Certified Security Practitioner

- Certified Information Systems Security Professional
- GIAC Firewall Analyst
- GIAC Incident Handler
- GIAC Intrusion Analyst
- GIAC Windows Security Administrator

Symantec Certified Security Engineer (SCSE)

Symantec Certified Security Engineer candidates must pass one of the following technology specialisation examinations:

- Virus protection and content filtering (Exam 250-201)
- Intrusion detection (Exam 250-202)
- Vulnerability management (Exam 250-203)
- Firewall and VPN technologies (Exam 250-204)

And all examinations in their chosen field of specialisation (two or three examinations). For a current list of product exams and their objectives please visit www.symantec.com.

Symantec Certified Security Practitioner (SCSP)

Symantec Certified Security Engineers may choose to progress to the highest level of Symantec certification and obtain the Symantec Certified Security Practitioner designation.

To achieve the SCSP certification candidates must already hold SCSE designation and pass all current Symantec product and technology specialisation examinations (currently 13 examinations are available – four technology and nine product specialisation examinations).

For an up to date list of examinations and their objectives please visit Symantec at www.symantec.com.

Symantec Product Specialist (SPS)

Symantec Product Specialists have in-depth knowledge of a particular Symantec solution. To achieve the Symantec Product Specialist designation candidates must pass one exam corresponding to their specialisation. The following specialisations currently exist:

- Virus protection and content filtering
- Intrusion detection
- Vulnerability management
- Firewall and VPN technologies

For a current list of existing product examinations and their objectives please visit Symantec at www.symantec.com. Symantec certification examinations are available at Prometric testing centres worldwide.

Symantec Technology Architect (STA)

Symantec Technology Architect candidates must pass one of the following security solutions examinations in order to achieve certification:

- Virus protection and content filtering (Exam 250-201)
- Intrusion detection (Exam 250-202)
- Vulnerability management (Exam 250-203)
- Firewall and VPN technologies (Exam 250-204)

Symantec certification examinations are available at Prometric testing centres worldwide. For up to date exam objectives please visit www.symantec.com.

About the Editor

Edgar Danielyan is a self-employed consultant, published author, technical editor and certified instructor specialising in information security, UNIX systems, and internetworking. With more than 10 years of work experience with government, international, non-profit and commercial organisations he is the founder and principal partner at Danielyan Consulting LLP, an information security consultancy providing information security solutions, consulting and training. His qualifications include Certified Information Systems Security Professional, TruSecure ICSA Certified Security Associate, CompTIA Security+, CCNP Security, CCDP, CSE Security, CIW Security Analyst, CIW Certified Instructor (Security), Sun Certified System and Network Administrator.

E-mail: danielyan@danielyan.com
WWW: www.danielyan.com

Detailed Table of Contents