APEC Guide to Information Security Skills Certification Booklet

www.siftsecurity.net

APEC Publication Number:
APEC#207-TC-03.1

APEC TEL
Security and Prosperity Steering Group

May 2007

Contents

Introduction

In the information security domain, certification programmes lend a level of credibility to a practitioner's experience and training, allowing managers to confidently determine the suitability of potential employees or service providers to an information security task.

This guide presents organisations and programmes which provide information security certification. By comparing certification knowledge areas and requirements, this guide helps practitioners[1] decide which certifications best match their career goals. For organisations, this guide provides information to help small-to-medium enterprises (SMEs) identify which certifications a professional[2] should hold to successfully perform the organisation's required duties.

USING THIS GUIDE

This intended reading order for this guide is as follows:

1. Read either the *Information for SMEs* or *Information for Individuals* depending on your situation
2. Use the *Certification Categories* section to create a shortlist of certifications
3. Consult the certification details section for full details of the certifications you are interested in.
4. Use the relevant appendices to compare certifications against 17799 and FIPS 200 standard.

About this Guide

The developers of the guide would like to thank the APEC Telecommunications Working Group (www.apectelwg.org) and the Australian Department of Communications, Information Technology and the Arts (www.dcita.gov.au) for supporting the development of this resource.

Information used in this resource was obtained from sources believed to be reliable. Certifications were catalogued in detail using publicly available information and were mapped objectively to vendor neutral standards. The information is correct at the time of publication, however SIFT accepts no liability for any errors that may have occurred in the production of this guide. Certification providers may contact SIFT through the related website to request updates to existing certification details or mappings, or to request new certifications be added to the database. For more information see the Providers sections of the related website.

[1] For the purpose of this guide practitioners are considered to be individuals who are seeking an information security certification.

[2] For the purpose of this guide professionals are a subset of practitioners who have already attained one (1) or more information security certifications.

WHAT ARE SECURITY CERTIFICATIONS?

Security certifications are accreditation programmes organised by a governing body to endorse a candidate's skill set, knowledge and core understanding of information security topics and technologies. The focus of each security certification varies greatly - from certifications targeting the implementation details of a specific security technology, to endorsing a candidate's holistic managerial knowledge of information security principles and practices.

Certifications are granted after candidates have satisfied a set of requirements, the number and depth of which varies depending on the scope of the certification. All certifications require candidates to pay a fee and pass a testing component - usually in exam or assignment format. The Information security knowledge required to gain certifications also varies considerably depending on the certification scope. While many certification programmes intend that the knowledge required to achieve accreditation is learnt through active experience, training programs to achieve certification are available, with either formal or informal relationships to the certification organisation themselves. Some certifications also have membership fees, ongoing knowledge development, and periodic retest requirements.

CERTIFICATION CLASSIFICATION

For the purposes of this project, information security certifications have been divided into two (2) main groups: independent certifications, and vendor certifications.

Independent certifications focus on security strategies, systems and technologies and are provided by organisations with no vendor affiliation. Rather than certify a practitioner's ability with specific controls for a given product range, vendor neutral certifications endorse a candidate's understanding of conceptual security knowledge and principles. With a few exceptions, independent certifications do not deal with specific brands or configuration controls for proprietary devices.

Vendor certifications cover a specific proprietary security technology or system, with certification usually requiring an in-depth knowledge and practice on the configuration and operation of these systems. As such, a wide range of vendor certifications exist, with each focusing on a specific security product. The examinations for vendor certifications are usually created by the proprietors of the system/technology. These certifications are most valid when a specific system/technology is known to be required by an organisation and in depth operational or applied knowledge is necessary to complete the required security task.

HOW THE CERTIFICATIONS WERE MAPPED

Certifications were mapped against two (2) broad security framework documents to better capture the differences between the independent certifications, and provide a means for individuals and SMEs to find certifications closely tailored to their needs. Mapping categories and tasks were extracted from the ISO IEC 17799:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management document, and the FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems.

ISO 17799 Mapping

The certifications were mapped against the ISO 17799 categories used in the APEC Information Security Awareness Guide. Certifications were noted to have either complete ©, partial (P) or no (N) coverage of each security function/task in the ISO 17799 mappings.

Complete (C) coverage denoted that security tasks that were covered by the certification to an in-depth level. Tasks that had been covered to a foundational or fundamental level were noted as partially covered (P). Where the certification had very little or no material on a security task or function, the certification was recorded to have no (N) coverage.

FIPS 200

Certifications were also mapped against the FIPS 200 categories used in the APEC Information Security Awareness Guide. The certifications were noted to have either complete (C), partial (P) or no (N) coverage of each security function/task in the FIPS 200 mappings.

Reference was made to the 'Specifications for Minimum Security Requirements' in the FIPS 200 document[3] to discern whether the certificate qualified as full or partial coverage for a given topic. Where the certification covered most or all of the described controls and functions for a listed category (eg, Access Control), the certification encompassed this category to complete (C) coverage. Where the certification only covered some of the listed controls, the certification was regarded to have partial (P) coverage. If the certification examined no information on the controls or functions, the certification had no (N) coverage.

[3] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Information for Small-to-Medium Enterprises (SMEs)

For SME organisations, information security certifications play a key role in the selection of professionals, vendors and consultancies to fill the company's security roles, or to help the organisation achieve and maintain compliance levels so as to be more marketable to clients or business partners. SMEs may also choose certifications for employees to undertake to ensure that employees can continue to fulfil their security related duties successfully.

Clear security goals should be defined prior to choosing any certified professionals to add into the SME's skill pool. These goals will define the job requirements, which inturn will mandate SME certifications that will be required by the organisation. When attempting to match security goals with certifications, SMEs should consider the following questions:

Questions for SMEs	Considerations
Is the motivation for security guidance due to current issues, or in order to prepare for the future?	When determining the scope of the security issues facing your organisation (and consequently the types of certified professionals required) SMEs should consider future IT strategy objectives.
Are you seeking a professional with a broad understanding of information security management or a technical specialist for a particular part of the security infrastructure?	Examine the certification "Type" and "Key Elements of Knowledge" to gain an understanding of what each certification covers so as to find the best fit to your business needs. Broadbase type certifications will cover a wider array of security concepts, whereas other certification types will provide a more focused approach.
Does the SME require certain types of systems/infrastructures audited?	If particular system types require auditing, SMEs should look towards certifications flagged under the "Auditing" type. Checking the "Key Elements of Knowledge" field and also the 17799 & FIPS mappings will help discern whether a certification covers a particular focus area. Tables in the Appendix map out certain broad technology types to various vendor certifications.
Are the technologies the acquired professional will be using well defined, and of a certain vendor? Does this vendor have a certification for the given technology?	If the answer is yes, check the vendor certification listing to see if that particular technology has a vendor certification. These certifications generally offer a more in-depth and technical approach to a specific brand of technology, and would be best for an SME in need of such specialised scoping. Tables in the Appendix map out certain broad technology types to various vendor certifications.
Do certifications verify a professional's technical competency?	Many of the independent certifications have technical styled questions in assessments which must be passed prior to becoming certified. However, this is not acceptable as a complete measure of technical competency. If a certification

	explicitly states that practical experience and / or training is required in order to gain certification, this will give better indication of a candidate's practical exposure.

SMEs must be aware that certifications do not necessarily guarantee technical competence. When searching for a candidate, other key criteria that indicate skill level and appropriateness for a given position should be highly factored into any selection processes.

Finally, the SME should ensure that any professionals under consideration are indeed certified as the claim. Governing bodies of certifications will generally have a service related to listing or finding professionals which are currently certified with them. These will generally be available on or through the governing body's websites or the certification's website.

Information for Individuals

There are 3 core reasons which drive people to seek further accreditation and certification in the information security field.

- To increase knowledge base
- To increase employability
- To increase remuneration

Knowledge base

Certifications consolidate a practitioner's ability, skill or knowledge in a particular topic focus, or a series of fundamental principles and concepts. Accordingly, practitioners can choose certifications which will develop or reinforce information security knowledge ranging from fundamental to advanced levels of depth, help them specialise in a particular field, or obtain a more holistic understanding of security topics and technologies.

Employability

In employment processes, when candidates are generally both equally well qualified in education and experience, certification can be the distinguishing factor to an employer. Granted that in many cases there are a large number of other key indicators that will affect the outcome of job applications, certification formally asserting the candidate's skill set is a distinct competitive advantage.

Remuneration

Generally, the more qualified a candidate is, the higher they can expect related remuneration packages to be. As an example, a 2007 survey taken by Global Knowledge identifies 15% difference between those with security certifications and those without[4].

CHOOSING A CERTIFICATION: GENERAL

The process of gaining a certification can require significant amounts of money and time. Hence, when choosing a certification, a series of factors must be taken into consideration. Initially, a practitioner should ask the following questions:

- Why do I wish to achieve certification?
- What is the area(s) of interest that I wish to certify in?
- Where is your current career path in IT security leading? Towards risk management, or towards the technical and operational side of information security?

For each certification that matches the initial criteria, further questions should be asked:

- How in-depth is the certification on the key areas of interest?

[4] Global Knowledge – "2007 IT Salary and Skills Report - What Impacts Salaries?" http://images.globalknowledge.com/wwwimages/pdfs/2007_SalaryReport.pdf

- How do you study for the certification? Is it self-study? Through external/internal training courses?
- How current and applicable is the certification?
- How widely recognised is the certification?
- How much does the certification cost?
- What bonuses are to be gained (salary-wise or otherwise) from gaining the certification?

CHOOSING A CERTIFICATION: STUDENTS

There are a number of foundational level security certifications suitable for Students and recent graduates wishing to enter the information security field, such as GISF, GOEC, GSEC, Security+ and TICSA. These certifications aim at providing the broad fundamental and conceptual base of security knowledge useful for gaining an entry level position within a company, or providing the education to shift from another area of IT operations into security.

More specific technical certifications may also be appropriate for students with an interest or job opportunity in a given topic area. However it is important to examine the experience requirements and assumed knowledge of each certification to ensure that it is a feasible undertaking – even if there are no official experience criteria imposed, a certification may require an applied knowledge of a certain IT environment or particular security product that is not practical for an individual to obtain alone.

CHOOSING A CERTIFICATION: IT SECURITY PRACTITIONERS

Seeking accreditation is a natural progression path in today's information security landscape. Certifications aid practitioners in signifying their technical skills and knowledge in mitigating current and emerging risks in information security. Managerial certifications also exist, which help practitioners move from technical oriented positions towards more managerial based security roles.

For practitioners who have just begun their career in information security, certifications can assist in their proof of knowledge base. Similarly, practitioners who seek extensive knowledge in a specific security topic or wish to learn a particular technology can indicate their specialised skills through certification. The post-nominals obtained through certification are valuable additions to a practitioner's title for the purpose of employability and corporate biographies.

Ultimately the desired career objectives of the individual should be the main consideration when choosing certifications. Initially it is recommended that individuals examine the security categories sections below, to obtain a list of security certifications which match their goals. By then examining the mapping of each candidate certification to 17799 and FIPS security tasks security practitioners can use this guide to identify which certifications best match their career objectives.

Certification Categories

To aid in selecting which certifications are most useful for your career or business need, certifications have been divided into categories based upon security tasks or technologies. These are:

- **Independent Certifications grouped by security tasks:**

  Independent Certifications are divided into the security tasks listed below. These refer to various duties that a SME might need fulfilled, or that an individual wishes to certify or strengthen their skill in.

- **Vendor Certifications grouped by security technologies:**

  Vendor certifications have been grouped by the category of security technology that the certification deals with. These certifications practitioner's ability in specific controls and concepts of a specific security technology or infrastructure.

Independent Certifications grouped by security tasks

Funtion	Description	Certification
Manage the security function	Certifications concerned with management level security processes and procedures, handling security issues from a business perspective and the management of the security function within an organisation.	CISM CISSP CPP GCSC ISSMP ISSPCS Practitioner
Design security processes and procedures	Certifications which require in-depth security knowledge across a range of security topics, for the purpose of designing security processes and procedures.	CISSP CPP GCSC I-RAP ISSAP ISSEP ISSPCS Practitioner
Information Security Auditing	Certifications concerned with IT security auditing of procedures and systems.	CIA CISA G7799 GSAE GSNA I-RAP
Business Continuity Planning	Certifications which certify practitioners in the area of business continuity planning, disaster recover and data backup operations.	CBCP/MBCP CPP I-RAP
Security Operations	Foundation level certifications which provide an introduction to security concepts, often covering a broad range of security topics.	GISF GOEC GSEC Security+ TICSA

Funtion	Description	Certification
Implement security technologies	Certifications which cover security topics at an applied level, typically focused on a specific technology or knowledge area.	GCFA GCFW GCIA GCIH GCWN GCUX GSIP ISSAP ISSEP SSCP

Vendor Certifications grouped by security technologies: (Vendor certifications are listed in full in Appendix C)

Funtion	Description	Certification
Secure application Design & Testing	Application security covering all stages of the development lifecycle.	MCAD MCSD
Network Infrastructure	The security of networking devices, technologies or architectures.	CCIE CCNA CCSP Cisco: - Information Security Specialist - VPN Specialist EnCE ECIE F5PC-FP JNCIA-SSL MCA:Infrastructure MCSA MCSE Nortel Certifications RSA Certifications
Firewalls	The configuration and deployment of firewalls.	Checkpoint Certifications CISCO Firewall Specialist CCSP JNCIA-FW JNCIA-FWV
Intrusion Detection/Prevention	The configuration and deployment of intrusion detection and intrusion prevention systems.	CCSP Cisco: - IPS Specialist - Security Solutions and Design Specialist ECIE ESSE JNCIA-IDP
Wireless	The security of wireless networks.	CWSP ECIE

Funtion	Description	Certification
System Hardening	The configuration of systems for increased security.	GCWN GCUX GSIP MCSA MCSE Novell Certified Linux Engineer RHCA RHCSS SAINT SCSECA SCSE SCSP SCTA SCTS
Forensics	Collection, analysis and recovery of electronic evidence.	EnCE

Independent Certifications

The section present a summary of all the certifications reviewed as part of this project. The sample shown in Appendix D: Explanation of Certification Details on page 87 explains what various fields and rating acronyms mean.

CBCP/MBCP (CERTIFIED BUSINESS CONTINUITY PROFESSIONAL)

DRI International (DRII)

http://www.drii.org/DRII/courses/certification_cbcp.aspx

Certification Description

The Certified Business Continuity Professional certification endorses a practitioner's knowledge of business continuity/disaster recovery concepts, processes and procedures. A CBCP is able to plan for realised business risks and threats, to safeguard interests of investors and other stakeholders. CBCPs are able to create awareness and training programmes for organisation staff to aid in any Business Continuity Plan.

The MBCP is a follow-on certificate to the CBCP. This certification certifies a practitioner's continued development in the Business Continuity profession (with a 5 year related industry experience requirement), and further in-depth knowledge on the key elements covered in the CBCP.

Experience Requirements

Two years of significant practical experience in five of the key elements.

Maintenance Requirements

CBCP/MBCP requires recertification every two years

Comply with DRII's Code of Ethics for Business Continuity Professionals.

Pay all annual maintenance fees.

Obtain a minimum number of continuing education points by submitting Continuing Education Points Reporting Forms to DRII on a regular basis.

Certification Type	Operations, Business Continuity
Applicability	• BCP professionals
Key Elements of Knowledge	• 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 • Crisis Communications • Coordination With External Agencies
Associated Code of Ethics	Not Applicable
Examination Format	Multiple-choice Questions
Post Nominal Gained	CBCP/MBCP
Country	USA
Cost	US$350 (CBCP)/ US$250 (MBCP) + application fees
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**C**	10.4 Protection Against Malicious and Mobile Code	**P**
6.1 Internal Organisation	**P**	10.5 Backup	**P**
6.2 External Parties	**C**	10.6 Network Security Management	**P**
8.2 During Employment	**C**	12.1 Security Requirements of Information Systems	**P**
9.1 Secure Areas	**C**	13.2 Management of Information Security Incidents and Improvements	**P**
9.2 Equipment Security	**P**	14.1 Information Security Aspects of Business Continuity Management	**C**
10.10 Monitoring	**P**	15.1 Compliance with Legal Requirements	**P**
10.3 System Planning and Acceptance	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**

FIPS 200 Mappings

Awareness and Training	**C**	Personnel Security	**C**
Certification, Accreditation, and Security Assessments	**P**	Physical and Environmental Protection	**P**
Contingency Planning	**C**	Planning	**C**
Incident Response	**P**	Risk Assessment	**C**
Media Protection	**P**	System and Services Acquisition	**P**

CIA (CERTIFIED INTERNAL AUDITOR)

Institute of Internal Auditors (IIA)

http://www.theiia.org/certification/certified-internal-auditor/

Certification Description

The Certified Internal Auditor certification asserts a candidate's ability to assess compliance, manage risk, and enforce privacy and physical security within the organisation. Network and system infrastructure review is covered at a high level in this certification.

Auditing of business functions is also covered in the CIA certification, including managerial accounting, financial accounting, strategic management, organisational behaviour and business processes.

Experience Requirements

Student candidates into the CIA program who are: (1) enrolled as a senior in an undergraduate program or as a graduate student; (2) full-time students as defined by the institution in which the student is enrolled (a minimum of 12 semester hours or its equivalent is required for undergraduate students and nine semester hours for graduate students); and (3) register for and take the CIA exam while enrolled in school.

24 months of internal auditing experience or its equivalent. (Those that passed the exam, but without experience, needs to get experience before certificate is issued.)

Maintenance Requirements

CIAs are required to maintain their knowledge and skills and to stay abreast of improvements and current developments in internal audit standards, procedures, and techniques.

Practicing CIAs must complete and report 80 hours of Continuing Professional Education (CPE) every two years.

Certification Type	Audit
Applicability	• Chief Audit Executives • Audit Managers • Audit Staff • Risk Management Staff • Educators • Students
Key Elements of Knowledge	• The Internal Audit Activity's Role in Governance, Risk, and Control • Conducting the Internal Audit Engagement • Business Analysis and Information Technology • Business Management Skills
Associated Code of Ethics	Code of Ethics established by The IIA
Examination Format	4 Exams, one for each topic area. 125 MC questions each 3 hours each
Post Nominal Gained	CIA
Country	USA
Cost	Unknown
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.6 Application and Information Access Control	**P**
5.1 Information Security Policy	**P**	11.7 Mobile Computing and Teleworking	**P**
6.1 Internal Organisation	**P**	12.1 Security Requirements of Information Systems	**P**
7.1 Responsibility for Assets	**P**	12.3 Cryptographic Controls	**P**
10.1 Operational Procedures and Responsibilities	**P**	12.5 Security in Development and Support	**P**
10.3 System Planning and Acceptance	**C**	12.6 Technical Vulnerability Management	**P**
10.6 Network Security Management	**P**	13.1 Reporting Information Security Events and Weaknesses	**P**
10.8 Exchange of Information	**P**	13.2 Management of Information Security Incidents and Improvements	**C**
10.9 Electronic Commerce Services	**C**	14.1 Information Security Aspects of Business Continuity Management	**P**
11.2 User Access Management	**P**	15.1 Compliance with Legal Requirements	**P**
11.4 Network Access Control	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**
11.5 Operating System Access Control	**P**	15.3 Information Systems Audit Considerations	**P**

FIPS 200 Mappings

Access Control	**P**	Media Protection	**P**
Audit and Accountability	**P**	Personnel Security	**P**
Awareness and Training	**P**	Planning	**P**
Certification, Accreditation, and Security Assessments	**P**	Risk Assessment	**P**
Contingency Planning	**P**	System and Communications Protection	**P**
Incident Response	**P**	System and Services Acquisition	**C**
Maintenance	**P**		

CISA (CERTIFIED INFORMATION SYSTEMS AUDITOR)

ISACA - The Information Systems Audit and Control Association & Foundation

www.isaca.org/cisa/

Certification Description

The Certified Information Systems Auditor certification endorses a candidate's understanding and knowledge of information auditing, controls and security. A CISA is able to audit and evaluate information systems and information systems security in a thorough and organised manner.

The focus of the certification is less on technical security (network and infrastructure) auditing, and more on systems auditing and compliance checking. Technical aspects are covered to some degree, but make up only a small part of the certification as a whole.

Experience Requirements

Complete five years work experience in the fields of Information Systems Auditing, Control, or Security.

Maintenance Requirements

Attain and report an annual minimum of twenty (20) continuing professional education hours.

Submit annual continuing professional education maintenance fees to ISACA international headquarters in full.

Attain and report a minimum of one hundred and twenty (120) continuing professional education hours for a three-year reporting period.

Respond and submit required documentation of continuing professional education activities if selected for the annual audit.

Certification Type	Audit
Applicability	• Information security auditors • Operational staff
Key Elements of Knowledge	• The IS Audit Process • IT Governance • Systems and Infrastructure Life Cycle Management • IT Service Delivery and Support • Protection of Information Assets • Business Continuity and Disaster Recovery
Associated Code of Ethics	ISACA Code of Professional Ethics
Examination Format	200 multiple-choice questions 4 Hours
Post Nominal Gained	CISA
Country	USA
Cost	ISACA Members: US $410 Nonmembers: US $530
ISO 17024 Accreditation	Yes

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.1 Business Requirement for Access Control	**C**
5.1 Information Security Policy	**C**	11.2 User Access Management	**P**
6.1 Internal Organisation	**P**	11.3 User Responsibilities	**P**
6.2 External Parties	**P**	11.4 Network Access Control	**P**
7.1 Responsibility for Assets	**P**	11.5 Operating System Access Control	**P**
8.1 Prior to Employment	**P**	11.6 Application and Information Access Control	**P**
8.2 During Employment	**P**	12.1 Security Requirements of Information Systems	**P**
9.1 Secure Areas	**P**	12.3 Cryptographic Controls	**P**
10.1 Operational Procedures and Responsibilities	**P**	12.4 Security of System Files	**P**
10.10 Monitoring	**P**	12.5 Security in Development and Support	**P**
10.2 Third Party Service Delivery Management	**P**	13.1 Reporting Information Security Events and Weaknesses	**C**
10.3 System Planning and Acceptance	**P**	13.2 Management of Information Security Incidents and Improvements	**P**
10.4 Protection Against Malicious and Mobile Code	**C**	14.1 Information Security Aspects of Business Continuity Management	**C**
10.5 Backup	**P**	15.1 Compliance with Legal Requirements	**P**
10.8 Exchange of Information	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**
10.9 Electronic Commerce Services	**P**	15.3 Information Systems Audit Considerations	**C**

FIPS 200 Mappings

Access Control	**P**	Personnel Security	**P**
Audit and Accountability	**C**	Physical and Environmental Protection	**P**
Awareness and Training	**P**	Planning	**P**
Certification, Accreditation, and Security Assessments	**P**	Risk Assessment	**P**
Contingency Planning	**C**	System and Communications Protection	**P**
Identification and Authentication	**P**	System and Information Integrity	**P**
Incident Response	**C**	System and Services Acquisition	**P**
Maintenance	**P**		

CISM (CERTIFIED INFORMATION SECURITY MANAGER)

ISACA - The Information Systems Audit and Control Association & Foundation

www.isaca.org/cism/

Certification Description

The Certified Information Systems Manager certification targets experienced information security managers or those with similar responsibilities. A CISM certification requires that the candidate has specific knowledge and business oriented skills in managing and overseeing organisational information security. The certification also covers designing, assessing, and technical security issues at a conceptual level.

Experience Requirements

Minimum of five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice analysis areas. Experience substitutes are available.

Maintenance Requirements

Annual maintenance fees.

Also attain and report an annual minimum of twenty (20) CPE hours and a minimum of one hundred and twenty (120) CPE hours for a three-year reporting period.

Certification Type	Management, Broadbase
Applicability	Experienced information security managers
Key Elements of Knowledge	• Information Security Governance • Information Risk Management • Information Security Program Development • Information Security Program Management • Incident Management and Response
Associated Code of Ethics	ISACA Code of Professional Ethics
Examination Format	200 multiple-choice questions 4 Hours
Post Nominal Gained	CISM
Country	USA
Cost	ISACA Members: US $410 Nonmembers: US $530
ISO 17024 Accreditation	Yes

17799 Mappings

4 Risk Assessment and Treatment	C	10.6 Network Security Management	P
5.1 Information Security Policy	C	11.1 Business Requirement for Access Control	C
6.1 Internal Organisation	P	12.1 Security Requirements of Information Systems	C
6.2 External Parties	C	12.3 Cryptographic Controls	P
7.1 Responsibility for Assets	P	12.5 Security in Development and Support	P
7.2 Information Classification	C	12.6 Technical Vulnerability Management	P
8.1 Prior to Employment	P	13.1 Reporting Information Security Events and Weaknesses	C
8.2 During Employment	C	13.2 Management of Information Security Incidents and Improvements	C
9.1 Secure Areas	P	14.1 Information Security Aspects of Business Continuity Management	C
10.1 Operational Procedures and Responsibilities	P	15.1 Compliance with Legal Requirements	P
10.10 Monitoring	P	15.2 Compliance with Security Policies and Standards, and Technical Compliance	C
10.2 Third Party Service Delivery Management	C	15.3 Information Systems Audit Considerations	P
10.5 Backup	P		

FIPS 200 Mappings

Access Control	P	Personnel Security	P
Audit and Accountability	P	Physical and Environmental Protection	P
Awareness and Training	C	Planning	C
Certification, Accreditation, and Security Assessments	P	Risk Assessment	C
Configuration Management	C	System and Communications Protection	P
Contingency Planning	C	System and Information Integrity	C
Incident Response	C	System and Services Acquisition	P

CISSP (CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL)

ISC 2 - International Information Systems Security Certification Consortium

https://www.isc2.org/cgi-bin/content.cgi?category=97

Certification Description

The CISSP certification tackles a very broad range of information security aspects and topics, covering managerial, operational and technical selections in the field. Both Technical and conceptual knowledge of the topics covered in the CISSP CBK is required to pass the exam, and indicates a minimum of adequate or greater knowledge and understanding of these areas in security.

The CISSP certification asserts practitioner's ability to design processes, policies and other standards for security measures rather than the ability to configure technical implementations, although best practice handling of many security issues is covered.

Candidates, who have not obtained the required years of related work experience, may obtain the Associate of (ISC)² certification by passing the CISSP Exam. Upon reaching the required years, an Associate of (ISC)² can receive their CISSP certification.

Experience Requirements

Have a minimum of four years of direct full-time security professional work experience in one or more of the ten domains of the (ISC)² CISSP® CBK® or three years of direct full-time security professional work experience in one or more of the ten domains of the CISSP® CBK® with a college degree.

Maintenance Requirements

Annual Fee.

Renew every 3 years via 120 Continuing Professional Education (CPE) credits.

Certification Type	Broadbase
Applicability	Mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.
Key Elements of Knowledge	• Access Control • Application Security • Business Continuity and Disaster Recovery Planning • Cryptography • Information Security and Risk Management • Legal, Regulations, Compliance and Investigations • Operations Security • Physical (Environmental) Security • Security Architecture and Design • Telecommunications and Network Security
Associated Code of Ethics	(ISC)2 Code of Ethics
Examination Format	250 multiple-choice questions 6 hours. Pass the CISSP exam with a scaled score of 700 points or greater.
Post Nominal Gained	CISSP
Country	USA
Cost	Early – US$499 Standard – US$599
ISO 17024 Accreditation	Yes

17799 Mappings

4 Risk Assessment and Treatment	C	10.8 Exchange of Information	C
5.1 Information Security Policy	C	10.9 Electronic Commerce Services	P
6.1 Internal Organisation	P	11.1 Business Requirement for Access Control	C
6.2 External Parties	P	11.2 User Access Management	C
7.1 Responsibility for Assets	C	11.3 User Responsibilities	C
7.2 Information Classification	C	11.4 Network Access Control	P
8.1 Prior to Employment	C	11.7 Mobile Computing and Teleworking	P
8.2 During Employment	C	12.1 Security Requirements of Information Systems	C
8.3 Termination or Change of Employment	C	12.2 Correct Processing in Applications	C
9.1 Secure Areas	C	12.3 Cryptographic Controls	C
9.2 Equipment Security	C	12.5 Security in Development and Support	C
10.1 Operational Procedures and Responsibilities	C	12.6 Technical Vulnerability Management	P
10.10 Monitoring	C	13.1 Reporting Information Security Events and Weaknesses	C
10.2 Third Party Service Delivery Management	P	13.2 Management of Information Security Incidents and Improvements	C
10.4 Protection Against Malicious and Mobile Code	C	14.1 Information Security Aspects of Business Continuity Management	C
10.5 Backup	C	15.1 Compliance with Legal Requirements	C
10.6 Network Security Management	C	15.2 Compliance with Security Policies and Standards, and Technical Compliance	C
10.7 Media Handling	C	15.3 Information Systems Audit Considerations	C

FIPS 200 Mappings

Access Control	C	Media Protection	C
Audit and Accountability	P	Personnel Security	C
Awareness and Training	C	Physical and Environmental Protection	C
Certification, Accreditation, and Security Assessments	P	Planning	C
Configuration Management	C	Risk Assessment	C
Contingency Planning	C	System and Communications Protection	C
Identification and Authentication	C	System and Information Integrity	P
Incident Response	C	System and Services Acquisition	P

CPP (CERTIFIED PROTECTION PROFESSIONAL)

ASIS

http://www.asisonline.org/certification/cpp/index.xml

Certification Description

The holder of a Certified Protection Professional certification must be able to plan and mitigate risks to personnel and assets in an organisation by developing, managing and evaluating policies, procedures and programs as methods towards protection.

The CPP has a large experience requirement of 9 years with at least three of those years managing the security function of an organisation. The CPP certification targets business and managerial knowledge and skill-sets in it's key knowledge elements.

Experience Requirements

Education: An earned bachelor's degree or higher from an accredited institution of higher education and work Experience: Seven (7) years of security experience, including at least three (3) years in responsible charge of a security function

OR

Work Experience: Nine (9) years of security experience, including at least three (3) years in responsible charge of a security function.

Maintenance Requirements

16 CPE credit points for 3 years term

Points system:
http://www.asisonline.org/certification/cpp/recertschedule.pdf

Certification Type	Broadbase	
Applicability	Experienced security professional	
Key Elements of Knowledge	• Security Management • Investigations • Legal Aspects (US, Canada and UK) • Personnel Security • Physical Security • Information Security • Business Principles & Practices • Protection of sensitive information • Emergency Management	
Associated Code of Ethics	Code of Professional Responsibility	
Examination Format	200 multiple-choice questions	
Post Nominal Gained	CPP	
Country	USA	
Cost	U.S. and Canada ASIS Member $300 Nonmember $450	International ASIS Member $200 Nonmember $350
ISO 17024 Accreditation	Full application	

17799 Mappings

4 Risk Assessment and Treatment	C	10.2 Third Party Service Delivery Management	C
6.1 Internal Organisation	C	10.5 Backup	P
6.2 External Parties	C	10.8 Exchange of Information	P
8.1 Prior to Employment	P	13.1 Reporting Information Security Events and Weaknesses	C
8.2 During Employment	C	13.2 Management of Information Security Incidents and Improvements	C
9.1 Secure Areas	P	15.1 Compliance with Legal Requirements	C
9.2 Equipment Security	P	15.2 Compliance with Security Policies and Standards, and Technical Compliance	P
10.10 Monitoring	P		

FIPS 200 Mappings

Audit and Accountability	P	Personnel Security	C
Awareness and Training	C	Physical and Environmental Protection	C
Contingency Planning	C	Planning	C
Incident Response	P	Risk Assessment	P
Maintenance	P		

G7799 (GIAC CERTIFIED ISO-17799 SPECIALIST)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/g7799.php

Certification Description

The holder of a GIAC Certified ISO-17799 Specialist certification must be able to assess and further the management of an organisation's security practices, procedures and processes, in adherence with the ISO-17799/27001 security framework. To become an accredited G7799 holder, the candidate will be able to demonstrate key risk management, security compliance, controls and process improvement knowledge as well as the ability to construct a 17799 compliant Information Security Management System.

SANS offers an associated course, AUDIT 411 – SANS 17799/27001 Security & Audit Framework, upon which the GIAC exam content is based. This includes forensic tool usage, data recovery, timeline analysis and network forensics.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Information security officers or other management professionals who are looking for a how-to guide for implementing ISO-17799 effectively
Key Elements of Knowledge	• Overview of ISO-17799 • Twelve Steps implementation process for ISO-17799 • SANS ISO-17799 Methodology
Associated Code of Ethic	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	G7799
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.6 Application and Information Access Control	**P**
5.1 Information Security Policy	**P**	11.7 Mobile Computing and Teleworking	**C**
6.1 Internal Organisation	**C**	12.1 Security Requirements of Information Systems	**P**
8.1 Prior to Employment	**C**	12.3 Cryptographic Controls	**P**
10.6 Network Security Management	**P**	12.4 Security of System Files	**C**
10.8 Exchange of Information	**P**	12.5 Security in Development and Support	**P**
11.1 Business Requirement for Access Control	**P**	14.1 Information Security Aspects of Business Continuity Management	**P**
11.2 User Access Management	**P**	15.1 Compliance with Legal Requirements	**P**
11.4 Network Access Control	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**
11.5 Operating System Access Control	**P**		

FIPS 200 Mappings

Access Control	**P**	Media Protection	**P**
Awareness and Training	**P**	Personnel Security	**C**
Certification, Accreditation, and Security Assessments	**P**	Planning	**P**
Contingency Planning	**P**	Risk Assessment	**P**
Incident Response	**P**		

GCFA (GIAC CERTIFIED FORENSIC ANALYST)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcfa.php

Certification Description

The GIAC Certified Forensics Analyst is a certificate targeting system administrators or people involved in incident handling. A GCFA holder must have a specialised knowledge in all matters of forensic analysis, from recovering data, retracing intrusion paths, evidence collection, and others.

SANS offers an associated course, SEC-508 – Systems Forensics, Investigation and Response, upon which the GIAC exam content is based. This includes forensic tool usage, data recovery, timeline analysis and network forensics.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals responsible for forensic investigation/analysis, advanced incident handling, or formal incident investigation.
Key Elements of Knowledge	• Core Forensic Filesystems Knowledge • Incident Response • Forensic Preparation • Windows Forensics • Unix and Linux 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
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GCFA
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

6.1 Internal Organisation	**P**	11.6 Application and Information Access Control	**P**
10.10 Monitoring	**C**	13.1 Reporting Information Security Events and Weaknesses	**P**
10.4 Protection Against Malicious and Mobile Code	**P**	13.2 Management of Information Security Incidents and Improvements	**P**
10.5 Backup	**P**	15.1 Compliance with Legal Requirements	**P**
10.6 Network Security Management	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**
10.8 Exchange of Information	**P**	15.3 Information Systems Audit Considerations	**P**
11.5 Operating System Access Control	**P**		

FIPS 200 Mappings

Audit and Accountability	**C**	Incident Response	**C**
Contingency Planning	**P**	System and Communications Protection	**C**

GCFW (GIAC CERTIFIED FIREWALL ANALSYT)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcfw.php

Certification Description

The GIAC Certified Firewall Analyst is a specialised certification which requires that a practitioner has in depth knowledge of network perimeter defence. It focuses on technologies such as:

- Packet Filters & Routers (incl. NAT and ACLs)
- Firewalls (rulesets, proxy gateways, log analysis)
- VPNs

GCFW asserts that a candidate can demonstrate the ability to design, configure, monitor and control these technologies. The associated SANS course, Security 502 – Perimeter Protection in Depth, covers all the material found in the GCFW certification exam.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals responsible for designing, implementing, configuring, and monitoring a secure perimeter for any organization; including routers, firewalls, VPNs/remote access, and overall network design.
Key Elements of Knowledge	• Design, configure, and monitor • Routers • Firewalls • VPNs/remote access • Overall network design • Perimeter defence systems
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit.
Post Nominal Gained	GCFW
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	P	10.8 Exchange of Information	P
10.10 Monitoring	P	11.4 Network Access Control	C
10.3 System Planning and Acceptance	P	11.7 Mobile Computing and Teleworking	C
10.4 Protection Against Malicious and Mobile Code	P	12.6 Technical Vulnerability Management	P
10.6 Network Security Management	P		

FIPS 200 Mappings

Configuration Management	P	System and Communications Protection	C
Planning	P	System and Information Integrity	P

GCIA (GIAC CERTIFIED INTRUSION ANALYST)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcia.php

Certification Description

The GIAC certified Intrusion Analyst certificate endorses that candidates posses an applied knowledge in intrusion detection systems, packet analysis and associated tools. Certification holders are able to analyse traffic and intrusion logs, and manage and configure related architecture.

SANS offers an associated course, SECURITY 503 – Intrusion Detection in Depth, upon which the GIAC exam content is based.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin, Technical
Applicability	Individuals responsible for network and host monitoring, traffic analysis, and intrusion detection.
Key Elements of Knowledge	• TCP/IP Security • Hands-On TCPdump Analysis • Hands-On Snort Usage • IDS Signatures and Analysis
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit.
Post Nominal Gained	GCIA
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	10.10 Monitoring	**P**
10.6 Network Security Management	**P**	11.4 Network Access Control	**P**
10.8 Exchange of Information	**P**	13.2 Management of Information Security Incidents and Improvements	**P**

FIPS 200 Mappings

Audit and Accountability	**C**	Incident Response	**P**
Certification, Accreditation, and Security Assessments	**P**	System and Information Integrity	**P**

GCIH (GIAC CERTIFIED INCIDENT HANDLER)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcih.php

Certification Description

The holder of a GIAC Certified Incident Handler certification must be able to manage incidents, understand common attack techniques and respond and/or defend against these. Candidates demonstrate some knowledge on designing, building and operating systems which prevent, defend or respond to these attacks. The certification asserts a technical competency in the subject area.

SANS offers an associated course, SECURITY 503 – Intrusion Detection in Depth, upon which the GIAC exam content is based

Experience Requirements

None

Maintenance Requirements

Renewal every 2 years

Certification Type	Security Admin, Operational
Applicability	Individuals responsible for incident handling/incident response; individuals who require an understanding of the current threats to systems and networks, along with effective countermeasures.[
Key Elements of Knowledge	• Understanding of the current threats to systems and networks • Effective countermeasures • Abilities to manage incidents • Understand common attack techniques and tools • Ability to defend against and/or respond to such attacks when they occur
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GCIH
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.5 Operating System Access Control	**P**
6.2 External Parties	**P**	11.7 Mobile Computing and Teleworking	**P**
10.4 Protection Against Malicious and Mobile Code	**C**	12.2 Correct Processing in Applications	**P**
10.5 Backup	**P**	12.6 Technical Vulnerability Management	**C**
10.6 Network Security Management	**P**	13.1 Reporting Information Security Events and Weaknesses	**P**
10.8 Exchange of Information	**P**	13.2 Management of Information Security Incidents and Improvements	**C**
10.9 Electronic Commerce Services	**P**	15.1 Compliance with Legal Requirements	**P**
11.3 User Responsibilities	**P**	15.3 Information Systems Audit Considerations	**P**
11.4 Network Access Control	**P**		

FIPS 200 Mappings

Access Control	**P**	System and Communications Protection	**P**
Incident Response	**C**	System and Information Integrity	**P**

GCSC (GIAC CERTIFIED SECURITY CONSULTANT)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcsc.php

Certification Description

The GIAC Certified Security Consultant certification is focused on business related skills rather than technical skills. These range from project planning and management, to evaluating and creating security policies and other deliverables, as well as various threat analysis techniques.

SANS offers an associated course, MGT-513 – Security Consultant, upon which the GIAC exam content is based. This includes forensic tool usage, data recovery, timeline analysis and network forensics.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals responsible for taking a leadership role in interfacing with clients and managing projects in a security consulting practice both technically and from a business perspective.
Key Elements of Knowledge	• Business personnel decisions • Understanding the impact of federal regulations • Project planning • Selling security services to clients • Evaluating and creating business continuity plans • Evaluating and creating security policies • Delivering the related technical details of security services within an organizations infrastructure
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GCSC
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.4 Network Access Control	**P**
5.1 Information Security Policy	**C**	11.7 Mobile Computing and Teleworking	**P**
6.1 Internal Organisation	**P**	12.1 Security Requirements of Information Systems	**P**
6.2 External Parties	**P**	12.2 Correct Processing in Applications	**P**
10.2 Third Party Service Delivery Management	**P**	14.1 Information Security Aspects of Business Continuity Management	**P**
10.4 Protection Against Malicious and Mobile Code	**P**	15.1 Compliance with Legal Requirements	**P**
10.6 Network Security Management	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**
10.8 Exchange of Information	**P**	15.3 Information Systems Audit Considerations	**P**
10.9 Electronic Commerce Services	**P**		

FIPS 200 Mappings

Awareness and Training	**P**	Planning	**P**
Certification, Accreditation, and Security Assessments	**P**	Risk Assessment	**C**
Configuration Management	**P**	System and Communications Protection	**P**
Contingency Planning	**P**	System and Information Integrity	**P**
Incident Response	**P**		

GCUX (GIAC CERTIFIED UNIX SECURITY ADMINISTRATOR)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcux.php

Certification Description

The GIAC Certified Unix Security Administrator certificate endorses that holders have demonstrated in-depth knowledge on securing Unix/Linux systems.
Content covered includes monitoring and alerting tools, network security, forensics, file system security, security administration and auditing systems.

SANS offers an associated course, SECURITY 506 – Securing Unix/Linux, upon which the GIAC exam content is based.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals responsible for installing, configuring, and monitoring UNIX and/or Linux systems.
Key Elements of Knowledge	• Secure and audit UNIX and Linux systems
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GCUX
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.2 User Access Management	**P**
9.2 Equipment Security	**P**	11.4 Network Access Control	**P**
10.10 Monitoring	**C**	11.5 Operating System Access Control	**P**
10.4 Protection Against Malicious and Mobile Code	**P**	11.6 Application and Information Access Control	**P**
10.6 Network Security Management	**C**	13.1 Reporting Information Security Events and Weaknesses	**P**
10.8 Exchange of Information	**P**	13.2 Management of Information Security Incidents and Improvements	**P**

FIPS 200 Mappings

Access Control	**P**	Incident Response	**C**
Audit and Accountability	**P**	Physical and Environmental Protection	**P**
Configuration Management	**C**	System and Communications Protection	**C**
Identification and Authentication	**P**	System and Information Integrity	**C**

GCWN (GIAC CERTIFIED WINDOWS SECURITY ADMINISTRATOR)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gcwn.php

Certification Description

Holders of the GIAC Certified Windows Security Administrator certificate must possess an in-depth knowledge of securing Windows 2000/XP/2003. This includes VPNs & IPSec, Group Policy, Active Directory, Digital Certificates, Encrypted File Systems and other Windows specific technologies.

SANS offers an associated course, SECURITY 505 – Securing Windows, upon which the GIAC exam content is based.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals responsible for installing, configuring, and securing Microsoft Windows 2000/XP/2003 networks.
Key Elements of Knowledge	• Secure and audit Windows systems • Group Policy • Active Directory • Internet Information Server • IPSec • Certificate Services
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GCWN
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.5 Operating System Access Control	**P**
10.10 Monitoring	**P**	11.6 Application and Information Access Control	**P**
10.6 Network Security Management	**P**	11.7 Mobile Computing and Teleworking	**P**
10.8 Exchange of Information	**P**	12.3 Cryptographic Controls	**C**
11.2 User Access Management	**P**	12.4 Security of System Files	**P**

FIPS 200 Mappings

Access Control	**P**	Media Protection	**P**
Audit and Accountability	**P**	Planning	**P**
Configuration Management	**P**	System and Communications Protection	**P**
Identification and Authentication	**P**	System and Information Integrity	**P**

GISF (GIAC INFORMATION SECURITY FUNDAMENTALS)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gisf.php

Certification Description

The GIAC Information Security Fundamentals certification is designed as an introduction to information assurance. This certification endorses a conceptual understanding of risk management, defence in depth, disaster recovery, business continuity and developing security policies. The GISF is listed on the GIAC site as a security administration certificate.

SANS offers an associated course, SECURITY 309 – Introduction to Information Security, upon which exam content is based.

Experience Requirements

None

Maintenance Requirements

Renewal every 2 years

Certification Type	Security Admin
Applicability	For Managers, Information Security Officers, and System Administrators who need an overview of information assurance.
Key Elements of Knowledge	• Risk management and defense in depth techniques • Disaster recovery or business continuity • Understanding the threats and risks to information • Identifying best practices • Diversify protection strategy
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GISF
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	P	10.10 Monitoring	P
5.1 Information Security Policy	P	11.1 Business Requirement for Access Control	P
6.1 Internal Organisation	P	11.2 User Access Management	P
6.2 External Parties	P	11.3 User Responsibilities	P
7.1 Responsibility for Assets	P	11.4 Network Access Control	P
7.2 Information Classification	P	11.5 Operating System Access Control	P
8.1 Prior to Employment	P	11.6 Application and Information Access Control	P
8.2 During Employment	P	11.7 Mobile Computing and Teleworking	P
9.1 Secure Areas	P	12.1 Security Requirements of Information Systems	P
9.2 Equipment Security	P	12.3 Cryptographic Controls	P
10.1 Operational Procedures and Responsibilities	P	13.1 Reporting Information Security Events and Weaknesses	P
10.4 Protection Against Malicious and Mobile Code	P	13.2 Management of Information Security Incidents and Improvements	P
10.6 Network Security Management	P	14.1 Information Security Aspects of Business Continuity Management	P
10.7 Media Handling	P	15.1 Compliance with Legal Requirements	P
10.8 Exchange of Information	P	15.3 Information Systems Audit Considerations	P
10.9 Electronic Commerce Services	P		

FIPS 200 Mappings

Access Control	P	Media Protection	P
Audit and Accountability	P	Physical and Environmental Protection	P
Contingency Planning	P	Planning	P
Identification and Authentication	P	Personnel Security	P
Incident Response	P	Risk Assessment	P

GOEC (GIAC OPERATIONS ESSENTIALS CERTIFICATION)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/goec.php

Certification Description

Correct use of operations is considered to intrinsically increase the security of an organisation. The GIAC Operations Essentials Certification endorses a candidate's operational competency in the planning, design, rollout and organisational procedures. This certification certifies business operation related skills and requires practical applied knowledge of the subject matter.

SANS offers an associated course, OPERATIONS 407 – Windows and Linux Service and Operations, upon which the GIAC exam content is based.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Data Center Managers, Operations Managers and Staff or anyone with System or Network experience
Key Elements of Knowledge	• Operations Fundamentals • Operations Models and Frameworks • Fundamental of TCP/IP Network • Packet Inspection • Network Architecture • Site Selection Process and Criterias • Power Issues • Heating and Ventilation • Rollout and Deployments • Network Troubleshooting • Performance Tuning • Service Level Agreements • Monitoring • Change Management • Asset and Configuration Management • Patch & Vulnerability Management • Backups • Securing Linux/Unix & Windows
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GOEC
Country	USA
Cost	With SANS Conference Training US$300
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	10.4 Protection Against Malicious and Mobile Code	**P**
7.1 Responsibility for Assets	**P**	10.5 Backup	**C**
9.1 Secure Areas	**P**	11.5 Operating System Access Control	**P**
9.2 Equipment Security	**P**	12.1 Security Requirements of Information Systems	**P**
10.1 Operational Procedures and Responsibilities	**P**	12.5 Security in Development and Support	**P**
10.10 Monitoring	**P**	12.6 Technical Vulnerability Management	**C**
10.2 Third Party Service Delivery Management	**P**	13.2 Management of Information Security Incidents and Improvements	**P**
10.3 System Planning and Acceptance	**C**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**

FIPS 200 Mappings

Configuration Management	**P**	System and Services Acquisition	**P**
Incident Response	**P**	System and Communications Protection	**P**
Physical and Environmental Protection	**P**	System and Information Integrity	**P**
Planning	**P**		

GSAE (GIAC SECURITY AUDIT ESSENTIALS)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gsae.php

Certification Description

The GIAC IT Security and Audit Essentials certification endorses the candidate's auditing knowledge in Networks and network related security, Physical security, Incident handling, Access control, Standards compliance.

SANS offers an associated course, AUD-410 - IT Security Audit & Control Essentials, upon which the GIAC exam content is based. This includes forensic tool usage, data recovery, timeline analysis and network forensics.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals entering the information security industry who are tasked with auditing organization policy, procedure, risk, or policy conformance.
Key Elements of Knowledge	• Host- and Network-based Intrusion Detection • Firewalls and Honeypots • Vulnerability Scanners • Computer Security Policies • Password Management • Incident Handling • Information Warfare • Encryption • Steganography • VPN's, PKI, and PGP
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GSAE
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	10.6 Network Security Management	**P**
5.1 Information Security Policy	**P**	11.1 Business Requirement for Access Control	**P**
6.1 Internal Organisation	**P**	11.2 User Access Management	**P**
7.1 Responsibility for Assets	**P**	11.5 Operating System Access Control	**P**
7.2 Information Classification	**P**	11.7 Mobile Computing and Teleworking	**P**
9.1 Secure Areas	**P**	12.3 Cryptographic Controls	**C**
10.10 Monitoring	**P**	13.1 Reporting Information Security Events and Weaknesses	**P**
10.4 Protection Against Malicious and Mobile Code	**P**	15.3 Information Systems Audit Considerations	**C**
10.5 Backup	**C**		

FIPS 200 Mappings

Access Control	**P**	Incident Response	**P**
Audit and Accountability	**P**	Media Protection	**P**
Certification, Accreditation, and Security Assessments	**P**	Physical and Environmental Protection	**P**
Identification and Authentication	**P**	Risk Assessment	**P**

GSEC (GIAC SECURITY ESSENTIALS CERTIFICATION)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gsec.php

Certification Description

The GIAC Security Essentials Certification examines and indicates fundamental knowledge of a large range of information security topics. Aimed at entry level professionals wishing to enter the industry or technical oriented management wishing to increase their understanding beyond conceptual levels, the GSEC certification is best suited to individuals seeking to demonstrate a solid grounding in information systems and networking security.

SANS offers an associated course, SECURITY 401 – SANS Security Essentials, which the GIAC upon which exam content is based.

Experience Requirements

None

Maintenance Requirements

Renewal every 2 years

Certification Type	Security Admin
Applicability	Security Professionals that want to fill the gaps in their understanding of technical information security and demonstrate they are qualified for hands on roles with IT systems with respect to security tasks.
Key Elements of Knowledge	• Networking Concepts • TCP/IP, Routing and Host Security • Network Security Overview • Information Warfare and Web Security • Internet Security Technologies, Network Vulnerabilities • Intrusion Detection and Risk Management • Introducing Encryption and Cryptography • PKI and Steganography • Secure Communications • Wireless Security • Windows Security • Windows XP Security and IIS Security • Backing up Windows and UNIX • Managing Software, System Services and Auditing • UNIX Security
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 100 multiple-choice questions and has a three hour time limit.
Post Nominal Gained	GSEC
Country	USA
Cost	US$800
ISO 17024 Accreditation	Full Application

17799 Mappings

4 Risk Assessment and Treatment	C	11.2 User Access Management	P
5.1 Information Security Policy	P	11.3 User Responsibilities	P
6.1 Internal Organisation	P	11.4 Network Access Control	P
6.2 External Parties	P	11.5 Operating System Access Control	P
7.2 Information Classification	P	11.7 Mobile Computing and Teleworking	C
9.1 Secure Areas	C	12.1 Security Requirements of Information Systems	C
9.2 Equipment Security	P	12.3 Cryptographic Controls	C
10.1 Operational Procedures and Responsibilities	P	12.4 Security of System Files	P
10.10 Monitoring	P	12.5 Security in Development and Support	P
10.5 Backup	C	12.6 Technical Vulnerability Management	P
10.6 Network Security Management	P	14.1 Information Security Aspects of Business Continuity Management	P
10.8 Exchange of Information	P	15.1 Compliance with Legal Requirements	P
11.1 Business Requirement for Access Control	C	15.3 Information Systems Audit Considerations	P

FIPS 200 Mappings

Access Control	P	Incident Response	P
Audit and Accountability	P	Media Protection	P
Awareness and Training	P	Personnel Security	P
Certification, Accreditation, and Security Assessments	P	Physical and Environmental Protection	C
Configuration Management	P	Planning	C
Contingency Planning	C	Risk Assessment	P
Identification and Authentication	P	System and Communications Protection	P

GSIP (GIAC SECURE INTERNET PRESENCE)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gsip.php

Certification Description

The GIAC Certified Secure Internet Presence certification is a specialised technical certificate, indicating a candidates ability to secure and audit LAMP system web applications. Technologies in the LAMP system include Linux, Apache, MySQL and PHP.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Security Admin
Applicability	Individuals responsible for installing, configuring, developing and monitoring secure web applications unsing Linux systems with Apache web server, MySQL databases and the PHP scripting language (LAMP)
Key Elements of Knowledge	• Secure and auditing skills in LAMP systems
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit
Post Nominal Gained	GSIP
Country	USA
Cost	Unknown
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.2 User Access Management	**P**
10.10 Monitoring	**P**	11.6 Application and Information Access Control	**P**
10.8 Exchange of Information	**P**	12.2 Correct Processing in Applications	**C**
10.9 Electronic Commerce Services	**C**		

FIPS 200 Mappings

Access Control	**P**	Media Protection	**P**
Configuration Management	**C**	System and Communications Protection	**P**
Identification and Authentication	**P**	System and Services Acquisition	**P**

GSNA (GIAC SYSTEMS AND NETWORK AUDITOR)

SANS – The SysAdmin, Audit, Network, Security Institute

http://www.giac.org/certifications/security/gsna.php

Certification Description

The GIAC Systems and Network Auditor certification asserts a practitioner's ability to auditing the security of networks and perform basic risk analysis, with specific technical auditing knowledge in the following areas:

- Routers
- Firewalls
- Wireless
- Databases
- Web based applications

SANS offers an associated course, AUDIT 507 – Auditing Networks, Perimeter & Systems, upon which the GIAC exam content is based. This includes forensic tool usage, data recovery, timeline analysis and network forensics.

Experience Requirements

None

Maintenance Requirements

Renewal every 4 years

Certification Type	Audit
Applicability	Technical staff responsible for securing and auditing information systems; auditors who wish to demonstrate technical knowledge of the systems they are responsible for auditing.
Key Elements of Knowledge	• Auditing Networks, Perimeters & Systems
Associated Code of Ethics	GIAC Code of Ethics
Examination Format	Two online exams, each exam contains 75 multiple-choice questions and has a two hour time limit.
Post Nominal Gained	GSNA
Country	USA
Cost	US$800
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.4 Network Access Control	**P**
10.10 Monitoring	**P**	11.7 Mobile Computing and Teleworking	**C**
10.2 Third Party Service Delivery Management	**P**	12.2 Correct Processing in Applications	**P**
10.6 Network Security Management	**P**	12.5 Security in Development and Support	**P**
10.8 Exchange of Information	**P**	15.3 Information Systems Audit Considerations	**P**
10.9 Electronic Commerce Services	**P**		

FIPS 200 Mappings

Access Control	**P**	Incident Response	**P**
Audit and Accountability	**P**	Planning	**P**
Certification, Accreditation, and Security Assessments	**P**	Risk Assessment	**P**
Configuration Management	**P**	System and Communications Protection	**P**
Identification and Authentication	**P**		

I-RAP (INFOSEC-REGISTERED ASSESSOR PROGRAMME)

SAI Global Professional Services

http://www.irap.securelink.com.au/

Certification Description

The Infosec-Registered Assessor Programme targets individuals wishing to work as an Australian government information security professional, in the field of security assessments. The I-RAP certification is a rigorous and thorough accreditation, covering many aspects of information security to a comprehensive and, where applicable, technical level. It is built on the Commonwealth Protective Security Manual (PSM) and the Australian Communications-Electronic Security Instruction 33, as well as key information system audit principles.

Experience Requirements

I-RAP demands twelve months of experience in relation to people who already have a 3-4 year IT degree, and experience in the field is required for I-RAP. Furthermore, the experience is assessed prior to the granting of examination eligibility. To get into the I-Rap program, DSD recommends that individuals have a broad range of commercial experience first.

Maintenance Requirements

The registration is valid for one year.

The mandatory requirements for registration renewal are:

Completion of update training presented by the I-RAP that will highlight any pertinent changes that have occurred since the initial training.

Review of the complaints and disputes records and any reviews of the assessor's work undertaken by the DSD during the period since the last assessment by the I-RAP administration in conjunction with the DSD.

Passing an assessment test presented by the I-RAP at the end of the training session.

Certification Type	Broadbase
Applicability	Government agency Information security professionals
Key Elements of Knowledge	• Commonwealth information security policy, including the Commonwealth Protective Security Manual (PSM) and the Australian Communications-Electronic Security Instruction 33 (ASCI 33) • I-RAP policy and procedural requirements • Aspects of Commonwealth information security requirements • Information system audit principles
Associated Code of Ethics	RAP rules
Examination Format	Unknown
Post Nominal Gained	I-RAP
Country	Australia
Cost	Application Fee $275.00 Applicant Training Fee $3,300.00 1st Year Annual License Fee $2,200.00
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	C	11.3 User Responsibilities	C
5.1 Information Security Policy	C	11.4 Network Access Control	C
6.1 Internal Organisation	P	11.5 Operating System Access Control	C
7.1 Responsibility for Assets	C	11.6 Application and Information Access Control	P
7.2 Information Classification	C	11.7 Mobile Computing and Teleworking	C
9.1 Secure Areas	P	12.1 Security Requirements of Information Systems	C
9.2 Equipment Security	C	12.2 Correct Processing in Applications	C
10.1 Operational Procedures and Responsibilities	C	12.3 Cryptographic Controls	C
10.10 Monitoring	P	12.4 Security of System Files	P
10.2 Third Party Service Delivery Management	P	12.5 Security in Development and Support	C
10.4 Protection Against Malicious and Mobile Code	C	13.1 Reporting Information Security Events and Weaknesses	C
10.5 Backup	C	13.2 Management of Information Security Incidents and Improvements	P
10.6 Network Security Management	C	14.1 Information Security Aspects of Business Continuity Management	C
10.7 Media Handling	C	15.1 Compliance with Legal Requirements	C
10.8 Exchange of Information	P	15.2 Compliance with Security Policies and Standards, and Technical Compliance	C
11.1 Business Requirement for Access Control	C	15.3 Information Systems Audit Considerations	C
11.2 User Access Management	C		

FIPS 200 Mappings

Access Control	C	Planning	C
Awareness and Training	C	Personnel Security	C
Audit and Accountability	C	Risk Assessment	C
Certification, Accreditation, and Security Assessments	C	System and Services Acquisition	C
Configuration Management	C	Contingency Planning	P
Identification and Authentication	C	Physical and Environmental Protection	P
Incident Response	C	System and Communications Protection	P
Maintenance	C	System and Information Integrity	P
Media Protection	C		

ISSAP (INFORMATION SYSTEMS SECURITY ARCHITECTURE PROFESSIONAL)

ISC 2 - International Information Systems Security Certification Consortium

https://www.isc2.org/cgi-bin/content.cgi?category=522

Certification Description

The Information Systems Security Architecture Professional (ISSAP) certification, asserts that, in addition to the knowledge gathered from the CISSP, participants are well qualified to design and implement secure information system architectures, and have specialised knowledge and skills in the following key knowledge categories listed for the ISSAP.

Experience Requirements

As per CISSP

Maintenance Requirements

Be a CISSP in good standing

Maintain the credential in good standing

Certification Type	Technical
Applicability	CISSPs
Key Elements of Knowledge	• Access Control Systems and Methodology • Telecommunications and Network Security • Cryptography • Requirements Analysis and Security Standards, Guidelines, Criteria
Associated Code of Ethics	(ISC)2 Code of Ethics
Examination Format	Pass the ISSAP examination
Post Nominal Gained	ISSAP
Country	USA
Cost	For two concentrations: Early Registration - US$ 599; Standard Registration - US$ 699) For three concentrations: Early Registration - US$ 749; Standard Registration - US$ 849)
ISO 17024 Accreditation	Yes

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.2 User Access Management	**C**
5.1 Information Security Policy	**P**	11.4 Network Access Control	**P**
9.1 Secure Areas	**C**	11.5 Operating System Access Control	**C**
9.2 Equipment Security	**C**	11.6 Application and Information Access Control	**C**
10.6 Network Security Management	**C**	11.7 Mobile Computing and Teleworking	**P**
10.8 Exchange of Information	**C**	12.3 Cryptographic Controls	**C**
11.1 Business Requirement for Access Control	**C**	14.1 Information Security Aspects of Business Continuity Management	**C**

FIPS 200 Mappings

Access Control	**C**	Media Protection	**P**
Audit and Accountability	**P**	Physical and Environmental Protection	**C**
Certification, Accreditation, and Security Assessments	**P**	Planning	**P**
Configuration Management	**P**	Risk Assessment	**P**
Contingency Planning	**C**	System and Communications Protection	**C**
Identification and Authentication	**C**	System and Information Integrity	**P**

ISSEP (INFORMATION SYSTEMS SECURITY ENGINEERING PROFESSIONAL)

ISC 2 - International Information Systems Security Certification Consortium

https://www.isc2.org/cgi-bin/content.cgi?category=523

Certification Description

The Information Systems Security Engineering Professional certification asserts that an individual has the technical and management skills to design and implement projects in a secure manner. The ISSEP has gained specialised and further knowledge in the systems security engineering related domains in addition to the CISSP body of knowledge.

Experience Requirements

As per CISSP

Maintenance Requirements

Be a CISSP in good standing

Maintain the credential in good standing

Certification Type	Technical
Applicability	CISSPs
Key Elements of Knowledge	• Systems Security Engineering • Certification and Accreditation • Technical Management • U.S. Government Information Assurance Regulations
Associated Code of Ethics	(ISC)2 Code of Ethics
Examination Format	Pass the ISSEP examination
Post Nominal Gained	ISSEP
Country	USA
Cost	For two concentrations: Early Registration - US$ 599; Standard Registration - US$ 699) For three concentrations: Early Registration - US$ 749; Standard Registration - US$ 849)
ISO 17024 Accreditation	Yes

17799 Mappings

4 Risk Assessment and Treatment	**P**	10.3 System Planning and Acceptance	**C**
5.1 Information Security Policy	**P**	12.1 Security Requirements of Information Systems	**C**
6.1 Internal Organisation	**P**	12.5 Security in Development and Support	**P**
10.2 Third Party Service Delivery Management	**P**	15.1 Compliance with Legal Requirements	**P**

FIPS 200 Mappings

Awareness and Training	**P**	Risk Assessment	**P**
Certification, Accreditation, and Security Assessments	**C**	System and Services Acquisition	**C**
Planning	**C**		

ISSMP (INFORMATION SYSTEMS SECURITY MANAGEMENT PROFESSIONAL)

ISC 2 - International Information Systems Security Certification Consortium

https://www.isc2.org/cgi/content.cgi?category=524

Certification Description

The Information Systems Security Management Professional certification endorses a practitioner's security expertise in management. In addition to the pre-requisite CISSP knowledge areas, candidates have honed their managerial skill-sets, with specific knowledge gained in enterprise wide security management and practices, overseeing compliance, business, disaster & operations continuity, planning and recovery, as well as legal and ethical considerations.

Experience Requirements

As Per CISSP

Maintenance Requirements

Be a CISSP in good standing

Maintain the credential in good standing

Certification Type	Management
Applicability	Holders of CISSP certificaiton
Key Elements of Knowledge	• Enterprise Security Management Practices • Enterprise-Wide System Development Security • Overseeing Compliance of Operations Security • Understanding Business Continuity Planning (BCP), Disaster Recovery Planning (DRP) and Continuity of Operations Planning (COOP) • Law, Investigations, Forensics and Ethics
Associated Code of Ethics	(ISC)2 Code of Ethics
Examination Format	Pass the ISSMP examination
Post Nominal Gained	ISSMP
Country	USA
Cost	For two concentrations: Early Registration - US$ 599; Standard Registration - US$ 699) For three concentrations: Early Registration - US$ 749; Standard Registration - US$ 849)
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**C**	10.6 Network Security Management	**P**
5.1 Information Security Policy	**C**	11.1 Business Requirement for Access Control	**C**
6.1 Internal Organisation	**P**	12.1 Security Requirements of Information Systems	**C**
6.2 External Parties	**C**	12.5 Security in Development and Support	**P**
7.2 Information Classification	**C**	12.6 Technical Vulnerability Management	**P**
8.1 Prior to Employment	**P**	13.1 Reporting Information Security Events and Weaknesses	**C**
8.2 During Employment	**C**	13.2 Management of Information Security Incidents and Improvements	**C**
10.1 Operational Procedures and Responsibilities	**P**	14.1 Information Security Aspects of Business Continuity Management	**C**
10.2 Third Party Service Delivery Management	**C**	15.1 Compliance with Legal Requirements	**P**
10.5 Backup	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**

FIPS 200 Mappings

Access Control	**P**	Personnel Security	**P**
Awareness and Training	**C**	Planning	**C**
Certification, Accreditation, and Security Assessments	**P**	Risk Assessment	**C**
Configuration Management	**P**	System and Communications Protection	**P**
Contingency Planning	**C**	System and Information Integrity	**P**
Incident Response	**C**	System and Services Acquisition	**P**

ISSPCS (THE INTERNATIONAL SYSTEMS SECURITY PROFESSIONAL CERTIFICATION SCHEME PRACTITIONER)

International Systems Security Engineering Association

http://www.isspcs.org/

Certification Description

The ISSPCS is currently an Australian based certification covering a broad range of information security topics, from managerial based concepts and knowledge bases, to functional disciplines relating to real applications of knowledge (eg, environmental and infrastructure security, systems security, communications and network security, physical security and personnel security).

The certification focuses on creating policies, procedures and processes for management of the various security areas covered in the certification, rather than in-depth configuration controls.

Experience Requirements

IT or related Degree (Bachelor or higher)

3 years information security experience

Maintenance Requirements

Certification last for 3 years

Certification Type	Broadbase
Applicability	Networking Operational staff to midlevel management
Key Elements of Knowledge	• Security Processes • Security Processes • Strategic Security Management • Compliance (Standards/Legal) • Asset Identification, Classification and Valuation • Security Risk Analysis and Assessment • Security Risk Treatment (Management of the Risk) • Operational Security Management • Security Operations: Normal Conditions • Security Operations: Abnormal Conditions • Functional Disciplines • Fundamental Theory
Associated Code of Ethics	ISSPCS Code of Ethics
Examination Format	4 hour closed book exam
Post Nominal Gained	ISSPCS Practitioner
Country	Australia
Cost	Australia exam + first 3 years AUD$500 + local taxes Australia 3 year recertification AUD$300 + local taxes Canada exam + first 3 years CAD$500 + local taxes Canada 3 year recertification CAD$300 + local taxes
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	C	10.6 Network Security Management	P
5.1 Information Security Policy	C	10.8 Exchange of Information	P
6.1 Internal Organisation	P	11.3 User Responsibilities	P
7.1 Responsibility for Assets	C	11.4 Network Access Control	P
7.2 Information Classification	C	12.1 Security Requirements of Information Systems	C
8.1 Prior to Employment	C	12.3 Cryptographic Controls	P
8.2 During Employment	C	12.5 Security in Development and Support	P
8.3 Termination or Change of Employment	C	13.2 Management of Information Security Incidents and Improvements	P
9.1 Secure Areas	C	14.1 Information Security Aspects of Business Continuity Management	C
9.2 Equipment Security	C	15.1 Compliance with Legal Requirements	C
10.1 Operational Procedures and Responsibilities	C	15.2 Compliance with Security Policies and Standards, and Technical Compliance	C
10.10 Monitoring	P	15.3 Information Systems Audit Considerations	C
10.2 Third Party Service Delivery Management	P		

FIPS 200 Mappings

Audit and Accountability	P	Media Protection	P
Awareness and Training	C	Personnel Security	C
Certification, Accreditation, and Security Assessments	P	Physical and Environmental Protection	C
Configuration Management	P	Planning	C
Contingency Planning	C	Risk Assessment	C
Incident Response	P	System and Communications Protection	P

SECURITY+ (COMPTIA SECURITY+ CERTIFICATION)

CompTIA

http://certification.comptia.org/security/

Certification Description

The Security+ certification is an entry-level broad certification which covers many aspects of information security. The exam focuses on conceptual levels of understanding for the majority of these topics, rather than any in-depth configuration or technical controls. Emphasis is placed on understanding various security technologies and how they can mitigate risks, or what actions can be taken to reduce risks in information systems and organisation security.

Experience Requirements

Two years experience in networking with emphasis on security.

CompTIA Network+ recommended, but not required.

Maintenance Requirements

None

Certification Type	Broadbase
Applicability	Individuals with a background in network and system admin
Key Elements of Knowledge	• General Security Concepts • Communications Security • Infrastructure Security • Encryption Technologies • Operational and Organizational Security
Associated Code of Ethics	None
Examination Format	100 questions Pass with 764 on a scale of 100 – 900 90 minutes
Post Nominal Gained	Security+
Country	USA
Cost	AUD$453.00
ISO 17024 Accreditation	Partial Application

17799 Mappings

4 Risk Assessment and Treatment	C	11.1 Business Requirement for Access Control	C
5.1 Information Security Policy	P	11.2 User Access Management	C
7.1 Responsibility for Assets	P	11.4 Network Access Control	P
8.3 Termination or Change of Employment	C	11.5 Operating System Access Control	P
9.1 Secure Areas	C	11.7 Mobile Computing and Teleworking	C
9.2 Equipment Security	P	12.3 Cryptographic Controls	C
10.10 Monitoring	P	12.4 Security of System Files	P
10.4 Protection Against Malicious and Mobile Code	C	12.5 Security in Development and Support	P
10.5 Backup	C	12.6 Technical Vulnerability Management	P
10.6 Network Security Management	C	13.1 Reporting Information Security Events and Weaknesses	P
10.7 Media Handling	C	13.2 Management of Information Security Incidents and Improvements	P
10.8 Exchange of Information	C	14.1 Information Security Aspects of Business Continuity Management	P
10.9 Electronic Commerce Services	P		

FIPS 200 Mappings

Access Control	C	Personnel Security	P
Configuration Management	C	Physical and Environmental Protection	C
Contingency Planning	C	Risk Assessment	P
Identification and Authentication	P	System and Communications Protection	P
Incident Response	P	System and Information Integrity	C
Media Protection	C		

SSCP (SYSTEMS SECURITY CERTIFIED PRACTITIONER)

ISC 2 - International Information Systems Security Certification Consortium

https://www.isc2.org/cgi-bin/content.cgi?category=98

Certification Description

The Systems Security Certified Practitioner credential targets an intermediate audience of security professionals, and focuses on the technical aspects of information security. The topics are covered both conceptually (network and telecommunications security and cryptography) and at an implementation or practical level (access control, analysis and monitoring, mitigating malicious code, risk, response & recovery and security operations & administration).

The certification can be used as a precursor to the CISSP qualification, as the SSCP covers a subset of the body of knowledge used in the CISSP certification, and with a lesser experience requirement. If a candidate does not have the required work experience for the SSCP, they may sit the exam, and remain an associate of the SSCP certification until they gain the required experience to receive full SSCP certification.

Experience Requirements

Applicants must have a minimum of one year of direct full-time security work experience in one or more of the seven domains of the (ISC)² SSCP® CBK.

Maintenance Requirements

Annual Fee.

Renew every 3 years via 60 Continuing Professional Education (CPE) credits

Certification Type	Broadbase
Applicability	Professionals working toward, or who have already attained, positions as Senior Network Security Engineers, Senior Security Systems Analysts or Senior Security Administrators.
Key Elements of Knowledge	• Access Control • Administration • Audit and Monitoring • Cryptography • Data Communications • Malicious Code / Malware • Risk, Response and Recovery
Associated Code of Ethics	(ISC)2 Code of Ethics
Examination Format	125 multiple-choice questions 3 hours Pass the SSCP exam with a scaled score of 700 points or greater.
Post Nominal Gained	SSCP
Country	USA
Cost	Early – US$369 Standard – US$469
ISO 17024 Accreditation	Yes

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.3 User Responsibilities	**P**
5.1 Information Security Policy	**P**	11.4 Network Access Control	**P**
6.1 Internal Organisation	**P**	12.1 Security Requirements of Information Systems	**P**
7.2 Information Classification	**C**	12.3 Cryptographic Controls	**C**
10.1 Operational Procedures and Responsibilities	**P**	12.6 Technical Vulnerability Management	**P**
10.10 Monitoring	**P**	13.1 Reporting Information Security Events and Weaknesses	**C**
10.4 Protection Against Malicious and Mobile Code	**C**	13.2 Management of Information Security Incidents and Improvements	**P**
10.5 Backup	**P**	14.1 Information Security Aspects of Business Continuity Management	**P**
10.6 Network Security Management	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**
11.1 Business Requirement for Access Control	**P**	15.3 Information Systems Audit Considerations	**P**
11.2 User Access Management	**C**		

FIPS 200 Mappings

Access Control	**P**	Personnel Security	**P**
Audit and Accountability	**P**	Planning	**P**
Certification, Accreditation, and Security Assessments	**P**	Risk Assessment	**P**
Configuration Management	**P**	System and Communications Protection	**P**
Contingency Planning	**C**	System and Information Integrity	**P**
Identification and Authentication	**P**	System and Services Acquisition	**P**
Incident Response	**C**		

TICSA (TRUSECURE ICSA CERTIFIED SECURITY ASSOCIATE)

TruSecure
https://ticsa.trusecure.com/

Certification Description

A TruSecure ICSA Certified Security Associate certification asserts the holder's foundational knowledge in a broad range of information security topics. The TICSA certification focuses on essential practices in information security and covers these to a conceptual level.

Experience Requirements

Have at least two years experience in network security administration, or can demonstrate attendance of at least 48 hours of approved computer security training or coursework

Maintenance Requirements

- Renewal every 2 years.
- 48 hours of approved educational or conference attendance, or evidence of equivalent
- Submit renewal fees

Certification Type	Broadbase
Applicability	• Network and computer systems administrators • Audit personnel • Other IT-oriented professionals.
Key Elements of Knowledge	• Security Practices and Procedures • Security Fundamentals • TCP/IP Networking Fundamentals • Firewall Management Fundamentals • Detection, Response & Recovery (I.R.) • Administration & Maintenance Fundamentals • Design & Configuration Basics • Malicious Code Fundamentals • Law, Ethics, and Policy • Authentication Fundamentals • Cryptography Basics • Fundamentals of Host-Based vs. Network-Based • Security • PKI and Digital Certificates • Fundamentals of OS Security
Associated Code of Ethics	TruSecure's Code of Ethics statement
Examination Format	• Approximately 70 multiple-choice • 90 mins
Post Nominal Gained	TICSA
Country	USA
Cost	• Domestic US$295.00 • International US$395.00
ISO 17024 Accreditation	No

17799 Mappings

4 Risk Assessment and Treatment	**P**	11.4 Network Access Control	**P**
5.1 Information Security Policy	**P**	11.5 Operating System Access Control	**P**
9.1 Secure Areas	**P**	11.7 Mobile Computing and Teleworking	**P**
9.2 Equipment Security	**P**	12.3 Cryptographic Controls	**P**
10.1 Operational Procedures and Responsibilities	**P**	12.4 Security of System Files	**P**
10.3 System Planning and Acceptance	**P**	12.6 Technical Vulnerability Management	**P**
10.4 Protection Against Malicious and Mobile Code	**P**	13.1 Reporting Information Security Events and Weaknesses	**P**
10.6 Network Security Management	**P**	13.2 Management of Information Security Incidents and Improvements	**P**
11.2 User Access Management	**P**	15.1 Compliance with Legal Requirements	**P**

FIPS 200 Mappings

Access Control	**P**	Physical and Environmental Protection	**P**
Configuration Management	**P**	Planning	**P**
Identification and Authentication	**P**	Risk Assessment	**P**
Incident Response	**P**	System and Communications Protection	**P**
Maintenance	**P**	System and Information Integrity	**P**
Media Protection	**P**		

Appendix A1: ISO 17799 Security Tasks Mapping (CBCP – GCWN)

Key	
●	Complete coverage of this security tasks against 17799
○	Partial coverage of this security tasks against 17799

17799 Security Tasks	CBCP/MBCP	CIA	CISA	CISM	CISSP	CPP	G7799	GCFA	GCFW	GCIA	GCIH	GCSC	GCUX	GCWN
4 Risk Assessment and Treatment														
4 Risk Assessment and Treatment	●	○	○	●	●	●	○		○	○	○	○	○	○
5 Security Policy														
5.1 Information Security Policy		○	●	●	●		○					●		
6 Organisation of Information Security														
6.1 Internal Organisation	○	○	○	○	○	●	●	○				○		
6.2 External Parties	●		○	●	○	●					○	○		

17799 Security Tasks	CBCP/MBCP	CIA	CISA	CISM	CISSP	CPP	G7799	GCFA	GCFW	GCIA	GCIH	GCSC	GCUX	GCWN
7 Asset Management														
7.1 Responsibility for Assets		○	○	○	●									
7.2 Information Classification				●	●									
8 Human Resources Security														
8.1 Prior to Employment			○	○	●	○	●							
8.2 During Employment	●		○	●	●	●								
8.3 Termination or Change of Employment					●									
9 Physical and Environmental Security														
9.1 Secure Areas	●		○	○	●	○								
9.2 Equipment Security	○				●	○							○	
10 Communications and Operations Management														
10.1 Operational Procedures and Responsibilities		○	○	○	●									
10.2 Third Party Service Delivery Management			○	●	○	●						○		

17799 Security Tasks	CBCP/MBCP	CIA	CISA	CISM	CISSP	CPP	G7799	GCFA	GCFW	GCIA	GCIH	GCSC	GCUX	GCWN
10.3 System Planning and Acceptance	○	●	○						○					
10.4 Protection Against Malicious and Mobile Code	○		●		●			○	○		●	○	○	
10.5 Backup	○		○	○	●	○		○			○			
10.6 Network Security Management	○	○		○	●		○	○	○	○	○	○	●	○
10.7 Media Handling					●									
10.8 Exchange of Information		○	○		●	○	○	○	○	○	○	○	○	○
10.9 Electronic Commerce Services		●	○		○						○	○		
10.10 Monitoring	○		○	○	●	○		●	○	○			●	○
11 Access Control														
11.1 Business Requirement for Access Control			●	●	●		○							
11.2 User Access Management		○	○		●		○						○	○
11.3 User Responsibilities			○		●						○			
11.4 Network Access Control		○	○		○		○		●	○	○	○	○	

17799 Security Tasks	CBCP/MBCP	CIA	CISA	CISM	CISSP	CPP	G7799	GCFA	GCFW	GCIA	GCIH	GCSC	GCUX	GCWN
11.5 Operating System Access Control		○	○				○	○			○		○	○
11.6 Application and Information Access Control		○	○				○	○					○	○
11.7 Mobile Computing and Teleworking		○			○		●		●		○	○		○
12 Information Systems Acquisition, Development and Maintenance														
12.1 Security Requirements of Information Systems	○	○	○	●	●		○					○		
12.2 Correct Processing in Applications					●						○	○		
12.3 Cryptographic Controls		○	○	○	●		○							●
12.4 Security of System Files			○				●							○
12.5 Security in Development and Support		○	○	○	●		○							
12.6 Technical Vulnerability Management		○		○	○				○		●			
13 Information Security Incident Management														
13.1 Reporting Information Security Events and Weaknesses		○	●	●	●	●		○			○		○	
13.2 Management of Information Security Incidents and Improvements	○	●	○	●	●	●		○		○	●		○	

17799 Security Tasks	CBCP/MBCP	CIA	CISA	CISM	CISSP	CPP	G7799	GCFA	GCFW	GCIA	GCIH	GCSC	GCUX	GCWN
14 Business Continuity Management														
14.1 Information Security Aspects of Business Continuity Management	●	○	●	●	●		○					○		
15 Compliance														
15.1 Compliance with Legal Requirements	○	○	○	○	●	●	○	○			○	○		
15.2 Compliance with Security Policies and Standards, and Technical Compliance	○	○	○	●	●	○	○	○				○		
15.3 Information Systems Audit Considerations		○	●	○	●			○			○	○		

Appendix A2: ISO 17799 Security Tasks Mapping (GISF – TICSA)

Key	
●	Complete coverage of this security tasks against 17799
○	Partial coverage of this security tasks against 17799

17799 Security Tasks	GISF	GOEC	GSAE	GSEC	GSIP	GSNA	I-RAP	ISSAP	ISSEP	ISSMP	ISSPCS Practitioner	Security+	SSCP	TICSA
4 Risk Assessment and Treatment														
4 Risk Assessment and Treatment	○	○	○	●	○	○	●	○	○	●	●	●	○	○
5 Security Policy														
5.1 Information Security Policy	○		○	○			●	○	○	●	●	○	○	○
6 Organisation of Information Security														
6.1 Internal Organisation	○		○	○			○		○	○	○		○	

17799 Security Tasks	GISF	GOEC	GSAE	GSEC	GSIP	GSNA	I-RAP	ISSAP	ISSEP	ISSMP	ISSPCS Practitioner	Security+	SSCP	TICSA
6.2 External Parties	○			○						●				
7 Asset Management														
7.1 Responsibility for Assets	○	○	○				●				●	○		
7.2 Information Classification	○		○	○			●			●	●		●	
8 Human Resources Security														
8.1 Prior to Employment	○									○	●			
8.2 During Employment	○									●	●			
8.3 Termination or Change of Employment											●	●		
9 Physical and Environmental Security														
9.1 Secure Areas	○	○	○	●			○	●			●	●		○
9.2 Equipment Security	○	○		○			●	●			●	○		○
10 Communications and Operations Management														
10.1 Operational Procedures and Responsibilities	○	○		○			●			○	●		○	○

17799 Security Tasks	GISF	GOEC	GSAE	GSEC	GSIP	GSNA	I-RAP	ISSAP	ISSEP	ISSMP	ISSPCS Practitioner	Security+	SSCP	TICSA
10.2 Third Party Service Delivery Management		○				○	○		○	●	○			
10.3 System Planning and Acceptance		●							●					○
10.4 Protection Against Malicious and Mobile Code	○	○	○				●					●	●	○
10.5 Backup		●	●	●			●			○		●	○	
10.6 Network Security Management	○		○	○		○	●	●		○	○	●	○	○
10.7 Media Handling	○						●					●		
10.8 Exchange of Information	○			○	○	○	○	●			○	●		
10.9 Electronic Commerce Services	○				●	○						○		
10.10 Monitoring	○	○	○	○	○	○	○				○	○	○	
11 Access Control														
11.1 Business Requirement for Access Control	○		○	●			●	●		●		●	○	
11.2 User Access Management	○		○	○	○		●	●				●	●	○
11.3 User Responsibilities	○			○			●				○		○	

17799 Security Tasks	GISF	GOEC	GSAE	GSEC	GSIP	GSNA	I-RAP	ISSAP	ISSEP	ISSMP	ISSPCS Practitioner	Security+	SSCP	TICSA
11.4 Network Access Control	○			○		○	●	○			○	○	○	○
11.5 Operating System Access Control	○	○	○	○			●	●				○		○
11.6 Application and Information Access Control	○				○		○	●						
11.7 Mobile Computing and Teleworking	○		○	●		●	●	○				●		○
12 Information Systems Acquisition, Development and Maintenance														
12.1 Security Requirements of Information Systems	○	○		●			●		●	●	●		○	
12.2 Correct Processing in Applications					●	○	●							
12.3 Cryptographic Controls	○		●	●			●	●			○	●	●	○
12.4 Security of System Files				○			○					○		○
12.5 Security in Development and Support		○		○		○	●		○	○	○	○		
12.6 Technical Vulnerability Management		●		○						○		○	○	○
13 Information Security Incident Management														
13.1 Reporting Information Security Events and Weaknesses	○		○				●			●		○	●	○

17799 Security Tasks	GISF	GOEC	GSAE	GSEC	GSIP	GSNA	I-RAP	ISSAP	ISSEP	ISSMP	ISSPCS Practitioner	Security+	SSCP	TICSA
13.2 Management of Information Security Incidents and Improvements	○	○					○			●	○	○	○	○
14 Business Continuity Management														
14.1 Information Security Aspects of Business Continuity Management	○			○			●	●		●	●	○	○	
15 Compliance														
15.1 Compliance with Legal Requirements	○			○			●		○	○	●			○
15.2 Compliance with Security Policies and Standards, and Technical Compliance		○					●			○	●		○	
15.3 Information Systems Audit Considerations	○		●	○		○	●				●		○	

Appendix B1: FIPS 200 Minimum Security Requirements Mapping (CBCP – GCWN)

Key	
●	Complete coverage of this security requirement against FIPS 200
○	Partial coverage of this security requirement against FIPS 200

FIPS 200 Minimum Security Requirements	CBCP/MBCP	CIA	CISA	CISM	CISSP	CPP	G7799	GCFA	GCFW	GCIA	GCIH	GCSC	GCUX	GCWN
Access Control		○	○	○	●		○				○		○	○
Awareness and Training	●	○	○	●	●	●	○					○		
Audit and Accountability		○	●	○	○	○		●		●			○	○
Certification, Accreditation, and Security Assessments	○	○	○	○	○		○			○		○		
Configuration Management				●	●				○			○	●	○
Contingency Planning	●	○	●	●	●	●	○	○				○		
Identification and Authentication			○		●								○	○
Incident Response	○	○	●	●	●	○	○	●		○	●	○	●	
Maintenance		○	○			○								
Media Protection	○	○			●		○							○
Physical and Environmental	○		○	○	●	●							○	

Protection														
Planning	●	○	○	●	●	●	○		○			○		○
Personnel Security	●	○	○	○	●	●	●							
Risk Assessment	●	○	○	●	●	○	○					●		
System and Services Acquisition	○	●	○	○	○									
System and Communications Protection		○	○	○	●			●	●		○	○	●	○
System and Information Integrity			○	●	○				○	○	○	○	●	○

Appendix B2: FIPS 200 Minimum Security Requirements Mapping (GISF-TICSA)

Key	
●	Complete coverage of this security requirement against FIPS 200
○	Partial coverage of this security requirement against FIPS 200

FIPS 200 Minimum Security Requirements	GISF	GOEC	GSAE	GSEC	GSIP	GSNA	I-RAP	ISSAP	ISSEP	ISSMP	ISSPCS Practitioner	Security+	SSCP	TICSA
Access Control	○		○	○	○	○	●	●		○		●	○	○
Awareness and Training				○			●		○	●	●			
Audit and Accountability	○		○	○		○	●	○			○		○	
Certification, Accreditation, and Security Assessments			○	○		○	●	○	●	○	○		○	
Configuration Management		○		○	●	○	●	○		○	○	●	○	○
Contingency Planning	○			●			○	●		●	●	●	●	
Identification and Authentication	○		○	○	○	○	●	●				○	○	○
Incident Response	○	○	○	○		○	●			●	○	○	●	○
Maintenance							●							○
Media Protection	○		○	○	○		●	○			○	●		○
Physical and Environmental	○	○	○	●			○	●			●	●		○

Protection														
Planning	○	○		●		○	●	○	●	●	●		○	○
Personnel Security	○			○			●			○	●	○	○	
Risk Assessment	○		○	○		○	●	○	○	●	●	○	○	○
System and Services Acquisition		○			○		●		●	○			○	
System and Communications Protection		○		○	○	○	○	●		○	○	○	○	○
System and Information Integrity		○					○	○		○		●	○	○

Appendix C: Vendor Certification Table

Key	
●	Covers this technology type
○	ISO 17024 - Has partially applied for 17024 certification

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
Check Point	Accelerated Check Point Certified Security Expert NGX (Accelerated CCSE NGX)				●					
Check Point	Check Point Certified Managed Security Expert NG with AI (CCMSE NG with AI)				●					
Check Point	Check Point Certified Managed Security Expert NG with AI Plus VSX (CCMSE NG AI Plus VSX)				●					
Check Point	Check Point Certified Managed Security Expert NGX (CCMSE NGX)				●					
Check Point	Check Point Certified Managed Security Expert NGX Plus VSX (CCMSE NGX Plus VSX)				●					

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
Check Point	Check Point Certified Master Architect				●					
Check Point	Check Point Certified Security Administrator NGX (CCSA NGX)				●					
Check Point	Check Point Certified Security Expert NGX (CCSE NGX)				●					
Check Point	Check Point Certified Security Expert Plus NG with AI (CCSE Plus NG with AI)				●					
Check Point	Check Point Certified Security Expert Plus NGX (CCSE Plus NGX)				●					
Check Point	Check Point Certified Security Principles Associate (CCSPA)				●					
Check Point	Check Point Certified Specialist - Integrity (CPIS)				●					
Cisco	Cisco Advanced Security Field Specialist			●						
Cisco	Cisco Certified Internetwork Expert (CCIE) Security			●						
Cisco	Cisco Certified Network Associate (CCNA)			●						○
Cisco	Cisco Certified Security Professional (CCSP)			●	●	●				○

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
Cisco	Cisco Firewall Specialist				●					
Cisco	Cisco Information Security Specialist			●						
Cisco	Cisco IPS Specialist					●				
Cisco	Cisco Security Solutions and Design Specialist			●		●				
Cisco	Cisco VPN Specialist			●						
CWNP	Certified Wireless Security Professional (CWSP)						●			
EnCase	EnCase Certified Examiner (EnCE)								●	
Enterasys	Enterasys Certified Internetworking Engineer (ECIE)			●		●	●			
Enterasys	Enterasys Security Systems Engineer (ESSE)			●		●				
F5	F5 Certified Product Consultant - FirePass (F5PC-FP)			●						
IBM	IBM Certified Advanced Deployment Professional - Tivoli Security Management Solutions 2006			●						

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
IBM	IBM Certified Advanced Security Professional - Notes and Domino 7			●						
IBM	IBM Certified Deployment Professional - Tivoli Federated Identity Manager V6.1			●						
IBM	IBM Certified Solution Advisor - Tivoli Security			●						
IBM	IBM Certified Specialist - Tivoli Identity Manager Express V4.6			●						
IBM	IBM Certified Specialist - Tivoli Monitoring Express V6.1			●						
Juniper	Juniper Networks Certified Internet Associate Firewall/VPN (JNCIA-FWV)				●					
Juniper	Juniper Networks Certified Internet Associate IDP (JNCIA-IDP)					●				
Juniper	Juniper Networks Certified Internet Associate SSL (JNCIA-SSL)			●						
Juniper	Juniper Networks Certified Internet Specialist Firewall/VPN (JNVIS-FWV)				●					
Microsoft	Microsoft Certified Application Developer (MCAD) with security specialisation		●							○
Microsoft	Microsoft Certified Architect (MCA): Infrastructure			●						

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
Microsoft	Microsoft Certified Architect (MCA): Solutions			●						
Microsoft	Microsoft Certified Solution Developer (MCSD) with security specialisation		●							○
Microsoft	Microsoft Certified Systems Administrator: Security (MCSA: Security)			●				●		○
Microsoft	Microsoft Certified Systems Engineer: Security (MCSE: Security)			●				●		○
Nortel Networks	Nortel Networks Certified Design Expert (NCDE) - Alteon Security			●	●					
Nortel Networks	Nortel Networks Certified Design Expert (NCDE) - Contivity Security			●						
Nortel Networks	Nortel Networks Certified Support Expert (NCSE) - Alteon Security			●						
Nortel Networks	Nortel Networks Certified Support Expert (NCSE) - Contivity Security			●	●					
Novell	Novell Certified Linux Engineer							●		
Red Hat	Red Hat Certified Architect (RHCA)							●		
Red Hat	Red Hat Certified Security Specialist (RHCSS)							●		

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
RSA	RSA Access Manager Certified Systems Engineer			●						
RSA	RSA Digital Certificate Management Solutions Certified Systems Engineer			●						
RSA	RSA SecurID Certified Administrator			●						
RSA	RSA SecurID Certified Instructor			●						
RSA	RSA SecurID Certified Systems Engineer			●						
RSA	RSA Sign-On Manager Certified Systems Engineer			●						
SAINT Corporation	SAINT							●		
Sourcefire	Snort Certified Professional (SnortCP)					●				
Sourcefire	Sourcefire Certified Expert (SFCE)					●				
Sourcefire	Sourcefire Certified Professional (SFCP)					●				
Sun Microsystems	Sun Certified Security Administrator (SCSECA) for the Solaris Operating System							●		

Provider	Certification	Technology Type	Secure application Design & Testing	Network Infrastructure	Firewalls	Intrusion Detection /Prevention	Wireless	System Hardening	Forensics	ISO 17024 Accredited
Symantec	Symantec Certified Security Engineer (SCSE)							●		
Symantec	Symantec Certified Security Practitioner (SCSP)							●		
Symantec	Symantec Certified Technology Architect (SCTA)							●		
Symantec	Symantec Certified Technology Specialist (SCTS)							●		

Appendix D: Explanation of Certification Details

Sample Certification Acronym (Sample Certification Full Name)

Sample Certification's Governing Body (DRII)

Sample Certification's website

Certification Description

These paragraphs contain a general overview of the certification. Included is a brief description of what skills or knowledge bases the certification endorses it's practitioners to have. Any information not captured in other sections (see below) will also be covered here.

Experience Requirements

A brief listing of any experience requirements required to obtain full accreditation for the certification.

Maintenance Requirements

A brief listing of any requirements required to maintain full accreditation by the certification body.

Certification Type	What type of accreditation this is (a certification can belong to more than one accreditation type): • Audit – includes financial, accounting, security and systems auditing • Management – Managing security functions and controls, helping an organisation work towards a more holistic security framework and approach. • Broadbase – Certifications which cover a wide range of security topics and functions (Minimum of 4 different security categories in ISO 17799). • Technical – Certifications which cover a technology or security practice to a technical level. This may range from configuration, building or an applied level of knowledge of the given task/security function. • Operational – An operational certification is one which endorses a practitioner's ability to operate security technologies, or with focuses on following procedures to better the security of an organisation. • Security Admin – Security administration certifications examine a practitioner's ability to control information security technologies and functions. This relates to roles such as network and systems administrators.
Applicability	A brief listing or paragraph concerning who should apply for this certification, or what sort of roles would benefit the most from this certification.
Key Elements of Knowledge	A listing of key knowledge elements covered in the certification exam.
Associated Code of Ethics	Listing of any codes of ethics followed/taught through the certification

Examination Format	Details on the examination format for the certification
Post Nominal Gained	Listing of any post nominals gained from the certification
Country	Country of origin
Cost	Associated costs with gaining the certification. This can include a separate (and annotated) cost of training.
ISO 17024 Accreditation	Either Yes, No, Full application, or Partial application, depending on whether the certification is ISO 17024 accredited or not (See Appendix E for further information).

17799 Mappings

This section has a tabulated form of the ISO 17799 mappings used to indicate what information is endorsed in a candidate by the certification (See Appendix D for further information about how we mapped the certifications). The certification will be noted to either have complete © or partial (P) coverage of each security function/task in the ISO 17799 mappings. If the certification has very little or no coverage of a particular security function/task, the function/task will not be included in this table (but will be included in Appendix A).

4 Risk Assessment and Treatment	**C**	10.4 Protection Against Malicious and Mobile Code	**P**
6.1 Internal Organisation	**P**	10.5 Backup	**P**
6.2 External Parties	**C**	10.6 Network Security Management	**P**
8.2 During Employment	**C**	12.1 Security Requirements of Information Systems	**P**
9.1 Secure Areas	**C**	13.2 Management of Information Security Incidents and Improvements	**P**
9.2 Equipment Security	**P**	14.1 Information Security Aspects of Business Continuity Management	**C**
10.10 Monitoring	**P**	15.1 Compliance with Legal Requirements	**P**
10.3 System Planning and Acceptance	**P**	15.2 Compliance with Security Policies and Standards, and Technical Compliance	**P**

FIPS 200 Mappings

This section has a tabulated form of the FIPS 200 Minimum Security Requirements mappings used to indicate what information is endorsed in a candidate by the certification (See Appendix D for further information about how the certifications were mapped). The certification will be noted to either have complete © or partial (P) coverage of each security technology/concept in the FIPS 200 mappings. If the certification has very little or no coverage of a particular security technology/concept, the technology/concept will not be included in this table (but will be included in Appendix A).

Awareness and Training	**C**	Personnel Security	**C**
Certification, Accreditation, and Security Assessments	**P**	Physical and Environmental Protection	**P**
Contingency Planning	**C**	Planning	**C**
Incident Response	**P**	Risk Assessment	**C**
Media Protection	**P**	System and Services Acquisition	**P**

Appendix E: How the certifications were mapped

Certifications were mapped against two (2) broad security framework documents to better capture the differences between the independent certifications, and provide a means for individuals and SMEs to find certifications closely tailored to their needs. Mapping categories and tasks were extracted from the ISO IEC 17799:2005 Information Technology – Security Techniques – Code of Practice for Information Security Management document, and the FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems.

ISO 17799 Mapping

The certifications were mapped against the ISO 17799 categories used in the APEC Information Security Awareness Guide. Certifications were noted to have either complete ©, partial (P) or no (N) coverage of each security function/task in the ISO 17799 mappings.

Complete (C) coverage denoted that security tasks that were covered by the certification to an in-depth level. Tasks that had been covered to a foundational or fundamental level were noted as partially covered (P). Where the certification had very little or no material on a security task or function, the certification was recorded to have no (N) coverage.

FIPS 200

Certifications were also mapped against the FIPS 200 categories used in the APEC Information Security Awareness Guide. The certifications were noted to have either complete (C), partial (P) or no (N) coverage of each security function/task in the FIPS 200 mappings.

Reference was made to the 'Specifications for Minimum Security Requirements' in the FIPS 200 document[5] to discern whether the certificate qualified as full or partial coverage for a given topic. Where the certification covered most or all of the described controls and functions for a listed category (eg, Access Control), the certification encompassed this category to complete (C) coverage. Where the certification only covered some of the listed controls, the certification was regarded to have partial (P) coverage. If the certification examined no information on the controls or functions, the certification had no (N) coverage.

[5] http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Appendix F: Validation of Certification Quality

In order to aid individuals and organisations in their certification related choices, a field on the certification's adherence to ISO/IEC 17024 has been included in the Information Security Certification Awareness Program.

Certification Programs which have not achieved full accreditation, but which are currently under application (either preliminary or full application), shall have this noted accordingly in the certification's listed details.

What is ISO/IEC 17024?

ISO/IEC 17024 is an international standard by ANSI for assuring that certification organisations adhere to a basis platform for delivering and continuing their certifications. For each certification that the organisation seeks accreditation for, the governing body of the certification will apply for initial eligibility and later, full application with ANSI, from which the certification will be approved or rejected for ISO/IEC 17024 compliance.

ISO/IEC 17024 will assess the certification body's policies and procedures, ensuring fairness and equity amongst candidates, compliance to applicable regulations and other controls listed in ISO/IEC 17024. ISO/IEC 17024 evaluates the following criteria for each certification:

- Development and maintenance of a certification scheme;
- A documented management system;
- Monitoring of subcontractors in the certification system;
- Maintenance of a record system;
- Confidentiality of information gained and security of examinations;
- The performance of resources, including examiners, employed by the certification bodies; and
- The re-certification process.

Appendix G: Other Links and Resources

Computer Security Resource Center (CSRC)	http://csrc.nist.gov/	Security standards, guidelines for security best practice
SANS	http://www.sans.org/free_resources.php http://www.incidents.org/	Security whitepapers, vulnerability information, security research and current internet threat information
W3C Web application Security	http://www.w3.org/Security/	
Forum of Incident Response and Security Teams	http://www.first.org/	Global Incident Response resources
Internet Engineering Task Force Security working group.	http://sec.ietf.org/	Internet security resources
Carnegie Mellon University's Computer Emergency Response Team.	http://www.cert.org/	Incident Response resources

Back Page

FOR THE ASIA-PACIFIC ECONOMIC COOPERATION SECRETARIAT

35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 6775-6012
Fax: (65) 6775-6013
Email: info@apec.org
Website: www.apec.org

Prepared By
SIFT Pty Ltd
Level 6, 62 Pitt Street Sydney NSW 2000 Australia
Tel: (61) 2 9236-7276
Fax: (61) 2 9251-6393
Email:apec@sift.com.au
Website: www.sift.com.au

APEC Publication Number:
APEC#207-TC-03.1