INFORMATION SECURITY SKILLS ACCREDITATION IN AUSTRALIA

The Current State and Industry Consensus on the Way Forward

FINAL VERSION FOR CIRCULATION
SIFT Pty Ltd
Date: November 2005

Table of Contents

Table of figures

1 Executive Summary

The purpose of this project was to examine the current information technology (IT) security qualifications available to Australian IT security professionals, to produce a 'state-of-play' report and to examine the need for, role and possible structure & governance arrangements of an IT security accreditation/certification scheme. This report includes a comprehensive review of the current industry and the views of individuals and organisations in industry and government regarding the need for an additional security skills accreditation or certification scheme.

SIFT Pty Ltd was awarded the consultancy to undertake the project.

Representatives from more than 40 stakeholder organisations contributed to this report through interviews, round table discussions and commentary during the course of the project and at an industry workshop sponsored by Department of Communications, Information Technology & the Arts (DCITA) held for this purpose. Contributors included:

- Accreditation and certification bodies;
- Industry associations for the information technology (IT), IT security, and information security industries[1];
- Consumers of information security professional services, including representatives from the banking and finance, telecommunications, Government, and utilities sectors;
- Bodies representing the interests of small to medium enterprises (SMEs);
- Representatives of universities and TAFE; and
- Organisations involved in the recruitment and placement of information security professionals.

The Australian information security community has more than 50 certification schemes available. These include industry recognised international schemes, vendor and product-specific certifications, Government-endorsed certification schemes and academic degrees and diplomas. The majority of information security qualifications currently available in Australia are owned, administered and regulated by overseas organisations.

Based on wide-ranging discussions with key stakeholders four main 'needs' were identified in the Australian information security skills marketplace. These needs are:

- the need for a mechanism to accurately assess competence;
- the need for information security professionals to possess greater knowledge;
- the need for professionals to possess knowledge and understanding specific to the Australian business environment; and
- the need for an informed market.

Discussions surrounding these 'needs' lead to the identification of a series of related points:

- To enable market forces for IT security skills to successfully operate, consumers of information security services and employers of information security professionals need to have access to information about skills available in the

1 The term "IT security" is considered to be a subset of information security.

market, including knowledge about existing qualifications and certifications and what these represent;

- Due to the global nature of the industry it is important that the qualifications, skills, knowledge and experience of Australian security professionals should continue to be recognised on an international level notwithstanding the value placed on specific Australian knowledge and experience by Australian consumers/employers;
- All practising security professionals should be able to access any new knowledge development activities, regardless of previous certification qualifications/certifications; and
- The majority of stakeholders consider that existing programs are meeting the industry's need to be able to accurately assess the competence of individuals with specific qualifications/certifications and there is no need to develop a new information security skills accreditation scheme for Australia.

A range of approaches were developed by the consultant and discussed with stakeholders. During discussions, a number of key principles emerged as crucial for the acceptance and success of any new approach to IT security skills accreditation. Any new approach should:

- build on existing certification programs;
- be open and recognise other international certifications already in existence as well as academic qualifications;
- minimise any additional costs to ensure value for money and accessibility;
- maintain vendor neutrality;
- be supported by both providers and consumers; and
- not be viewed by consumers/employers as a substitute for due diligence in verifying the qualifications, skills and knowledge of potential contractors/employees.

Industry Workshop

A workshop was held in June 2005 in Sydney to inform stakeholders of the consultant's stage 1 findings and to present five possible approaches for a way forward. All individuals/organisations interviewed for the first stage of the report were invited to the workshop. The options put forward to workshop participants were:

- Market forces: To continue to allow the direction of accreditation and certification in Australia to be determined by industry market forces.
  - Workshop participants reacted positively towards the current certification programs which have evolved due to market forces, and acknowledged the continuing work by certification bodies to meet the changing and developing needs of industry.
- Licensing and registration: Information security professionals could be required to register with a licensing program in order to practise in the industry.
  - Workshop participants were opposed to the introduction of a mandatory licensing and registration scheme, and without industry support it was agreed that the model should not be pursued further.

- Program accreditation: An accreditation scheme for certification providers could be established. Participants discussed existing mechanisms for accrediting certification bodies, including ISO/IEC 17024-2004: Conformity Assessment – General requirements for bodies operating certification of persons.
  - As participants noted that certification providers, rather than individual professionals can already obtain accreditation to international standards, to ensure the quality and integrity of certification programs this approach was not pursued further.
- Awareness program: An information program could be developed to assist organisations and professionals understand the range, relevance and content of IT security qualifications available in Australia.
  - Workshop participants indicated strong support for an awareness program to provide information to both security professionals and consumers/employers of security services, on certifications available to the Australian market. Participants discussed how such a program could encompass a *Buyers' Guide* describing the range of qualifications held by IT security professionals in Australia. It was noted that to be viable this program would need to be supported by both certification providers, academic institutions and the consumer/employers of IT security services.
- Consumer protection: Standard form contracts for common IT security services could be developed to improve the quality and consistency of services provided by professionals.
  - It was suggested by some participants that consumer law could afford some protection for organisations, particularly for SMEs acquiring information security services. There was however agreement that standard form contracts alone could not ensure that professionals were able to meet individual organisation's requirements.
  - It was noted that the utility of consumer protection mechanisms, such as standard form contracts was minimal as large consumers/employers of information security professional services would generally already use internal legal and compliance personnel and associated contracts.

Participant's Conclusions

- Market forces will determine the need for new Australian certification programs

When presented with the consultant's findings and potential models, the majority of participants agreed that current certification programs are meeting industry requirements and there is neither a compelling need, nor a compelling driver for the creation of a new Australian certification program.

- Current certification programs can be used by buyers as a benchmark

Participants had differing views on the state of accreditation in Australia but generally conceded that current certification programs are valuable as a benchmark as they demonstrate a professional's degree of understanding, dedication and discipline in the industry. It was agreed that any gaps between certification programs and industry standards

were a reflection of the different targets set by each program and the rapidly changing needs of consumers and employers.

- Some gaps do exist between the supply of professionals & the demand for services

Participants agreed that there was scope for further discussion on whether existing certifications could be enhanced in light of gaps identified by the project.[2]

An Australian training component

An Australian training component was proposed as a solution to address the lack of regional knowledge faced by professionals who practise in the Australian information security environment. The Australian IT Security Training Component would include relevant domestic issues and inform information security professionals on Australian legislation and regulation requirements, such as the Privacy Act and Australian telecommunications legislation.

Such a component would be offered as an additional option within existing certification and qualification schemes available in Australia.

It was emphasised by participants that the purpose of the Australian training component would be to create a reference level of knowledge and not to train information security professionals to become 'legal experts'. It was accepted that professionals should have an understanding and awareness of Australia's legal and regulatory environment in order to practise information security within legal boundaries.

Awareness of Certification Programs

Participants agreed that consumers/employers of information security services needed to be better informed as to what existing certifications represent. It was observed that many consumers/employers of IT Security services do not understand the relative positioning of existing programs, nor are they able to identify the different skill sets of professionals holding different certifications.

There was broad stakeholder agreement that consumers/employers also need general assistance to be able to accurately assess the competence of specific individuals.

To achieve this objective a number of organisations proposed the concept of a Buyer's Guide as the medium for information on programs. However, it was acknowledged that a Buyer's Guide could not be expected in one stroke to solve all information issues in the industry. It was agreed that all the following items would provide valuable information to both consumers/employers of information security services and information security professionals themselves.

1. An explanation of the differences between IT security and information security.
2. Descriptions of common roles and responsibilities for job roles within the information security industry.
3. A list of qualifications including information security programs offered by certification bodies, various educational institutions and universities. Content should be easily comprehensible and should summarise the skills and knowledge

2 As the objective of this project was to determine both stakeholder acceptance and possible governance arrangements for an IT security skills accreditation/certification scheme, options for possible governance structures were canvassed with representatives interviewed. The industry consensus was that no new scheme should be developed; these structures are discussed briefly in the full report, but not in the Executive Summary.

examined as well as the requirement for continuing professional education by each qualification.

4. A guide as to the technical abilities and management skills covered by each qualification. It should also suggest which certifications could match specific job roles.
5. An explanation of the ISO/IEC 17024 international accreditation standard and its role in providing a quality assurance benchmark for certification bodies.
6. A directory of contacts for each qualification provider and relevant industry associations.

It was agreed that a Buyers' Guide could:

- Provide an accepted point of reference with which to compare and contrast certification schemes currently available;
- Increase the confidence level of consumers in knowing when help is required for information security;
- Provide information on how to select the appropriate information security professional for the job;
- Inform consumers and professionals and allow them to select the most appropriate program for their needs; and
- Include pointers to relevant standards and methodologies.

The Way Forward

In summary, participants representing a wide range of interests, were keen to continue to encourage certification providers to respond to market forces, while supporting the development of two initiatives, being:

- An IT Security Accreditation Awareness Program (including an IT Security Buyer's Guide); and
- An Australian IT Security Training Component.

The Department of Communications, Information Technology & the Arts proposes that:

- this report be widely circulated to all participants;
- the Department convene a group of interested industry and government agencies to determine:
  - if there is broad agreement in the project's conclusions; and
    - if there is sufficient interest in the concept of an IT security awareness program including a Buyers' Guide to be developed and funded by industry; and
    - if there is market support for an Australian IT security component.

November
2005

2 PROJECT BACKGROUND & CONTEXT

2.1 DEFINITIONS

IT security is considered to be a subset of information security, although for the purpose of this project, the terms were considered to be interchangeable on the basis that the two professions have similar skill accreditation concerns.

The term "IT security skills" refers to the necessary competencies a professional would require to appropriately and successfully secure an organisation's IT systems.

"Information security skills" incorporates a slightly broader definition, referring to the necessary competencies a professional would require to appropriately and successfully secure an organisation's information, whether within an IT system or elsewhere.

It is acknowledged that the level and type of skills required in these fields will differ markedly between job roles and organisation types.

2.2 BACKGROUND

The demand for information security professionals has continued to grow both in the public and private sectors over recent years. Information Security Interest Group (ISIG) Secretary Mark Ames has estimated that there are between 1000 and 2000 information security professionals currently working in Australia [LeMay 2005b].

In addition, there are a wide range of ICT professionals with considerable exposure to the security field. The current marketplace offers a range of qualifications, from vendor and product-specific certifications and internationally administered broad-based qualifications, to academic degrees and diplomas.

There has been ongoing discussion within industry associations on the need to develop a qualification tailored to the Australian marketplace. It was believed that such a scheme would establish a common acceptable denominator – but not a lowest common denominator – for information security practitioners and would allow for greater consumer choice and service [Ames, Gaskell & Muir 2003].

The issue of information security skills accreditation has received recognition at an international level, including through the Asia-Pacific Economic Co-operation (APEC) and International Federation for Information Processing (IFIP) forums.

IFIP Technical Committee 11 (Privacy and Security in Information Processing Systems) released the following statement on Information Security Professionals at the 2002 annual meeting in Cairo, Egypt:

TC-11 requests all member societies of IFIP to urge their relevant government and education bodies to ensure that proper education and certification requirements are set for those people who intend to become information security professionals and including those who audit the security of IT systems.

In particular, TC-11 recommends that:

- Minimum education and training requirements be set for any such professionals;
- Any such minimum educational and training requirements should reflect similar standards in life professionals; and
- Such education and training professionals be developed in line with emerging international standards in the area of information security. [IFIP 2002]

The aim of this project was to evaluate the need for an Australian information security skills accreditation scheme, and subsequently to summarise industry views on the way forward [DCITA 2005]. The report combines findings derived from published literature, outcomes from discussion held with key stakeholders and the examination of potential models for supporting this area.

2.3 LOCAL CONTEXT

A number of advocates have suggested that there is a need for an Australian qualification to cater for local security issues, legislation and corporate governance requirements [LeMay 2005a]. Professor Vijay Varadharajan, Director of the ACS Computer Science Board and Professor in Computing at Macquarie University, has indicated that as the demand for ICT security professionals increases in the public and private sectors, there is a need for a method of measurement to certify security professionals in terms of their qualifications and experience [Varadharajan 2004].

In 2003, ISIG released a discussion paper on the topic of certification. ISIG concluded that a "national professional registry of information security professionals should be established in consultation with Commonwealth and State Governments and industry organisations". Furthermore, ISIG suggested a "certification scheme should be integrated with the registration process. That is to say, only persons who meet skills-based requirements should be registered under this scheme". [Ames, Gaskell & Muir 2003]. ISIG suggested that the necessary core components for the certification scheme should include:

- General knowledge of information security principles based on ISO/IEC AS/NZS 17799 and AS/NZS 7799.2; and
- General knowledge of Australian legal and regulatory requirements, including state and federal laws, regulations, and standards [Ames, Gaskell & Muir 2003].

The development of a localised component for professional certifications has seen little progress since it was recommended in the 2003 ISIG paper.

The Australian Computer Society (ACS) launched a bid in October 2004 to become the main accreditation body for the Australian IT industry. In the launch the ACS argued for powers similar to other industry organisations, such as the state bar association in the legal profession [Jenkins 2005].

The Australian IT Security Forum (AITSF) has commented that the debate on information security skills accreditation is still unresolved. AITSF and ISIG declared their joint position on this topic in March 2005. Their position is characterised as follows:

A multitude of (international) certification schemes for information security professionals is already established.

An additional Australian scheme is neither desirable nor feasible.

We (AITSF) do not have a comprehensive picture of what the various stakeholders expect from certification schemes.

We (AITSF) believe that the various stakeholders themselves do not have a comprehensive picture of what to expect from certification schemes. [AITSF 2005]

2.4 INTERNATIONAL CONTEXT

Given the breadth of the field of information security, it is not surprising that there are differing views on the required knowledge for a 'professional' in this area. Most agree that core elements such as confidentiality, availability and integrity of information belong in the discipline, while the inclusion of elements such as business continuity / disaster recovery planning, insurance, fraud prevention and physical security of information assets and physical documents have been questioned at times [ISPWG 2004].

While industry certifications have received criticism for their use of examinations as the primary assessment mechanism, criticism has also been levelled at academic qualifications for omitting a relevant work experience requirement. This element is seen by APEC as a critical component of information security skills development. The APEC IT Skills Report tabled in 2004 states, "there is a role for APEC to ensure that IT skills development involves an appropriate balance of theoretical and practical work" [APEC 2004].

According to a 2004 draft APEC e-Security skills report, of all APEC nations, only Japan has a national scheme specifically aimed at accrediting information security professionals. [APEC 2004].

In 2003, the European Information Society Group (EURIM) considered the training requirements of law enforcement and industry in order to tackle e-crime. The EURIM report states, "only with formal accreditation are qualifications likely to be seen as having worth." [EURIM 2003].

Following is a brief summary of international activity in the area of information security skills accreditation

2.4.1 Japan

Japan has implemented a number of schemes in the area of information security skills accreditation, with each intended for a clear audience and use:

- Qualification Examination for Chief Telecommunications Engineers;
- Network Information Security Manager (NISM);
- Information Security Administrator Examination;
- Qualification Test for Chief Evaluator of Security Target; and
- Information Security Management System Auditor.

[APEC 2004]

Japan implemented these schemes to encourage the alignment to international standards (namely ISO/IEC 17799 and BS 7799.2). Subsequent to these schemes being put in place, and claimed as evidence of the program's success, 500 organisations have been certified against these internationally recognised information security standards. [HKCS 2004]

2.4.2 United States of America

The US Government has not created its own certification scheme for information security professionals. Instead, it requires individuals working in specific government information security positions to obtain a commercially available information security certification [Williamson, (ISC)^2 2005].

For example, the US Department of Defence (DoD) is expected to issue an "implementing manual" to accompany an existing DoD Directive, which will require approximately 110,000 DoD employees and contractors to obtain one of a number of specified commercially-available information security certifications as a condition for their continued employment in information assurance and information management-related positions. The Directive identifies six defined categories of personnel (Technical I, II and III; and Management I, II, and III), with each position having a required level of certifications, with the accepted certifications required to be ISO/IEC 17024 accredited [(ISC)^2 2005c].

The US National Security Agency (NSA) and the US Department of Homeland Security (DHS) have jointly developed a program to support the US National Policy on Critical Infrastructure Protection (Presidential Decision Directive 63). The US National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program is responsible for the accreditation of information security programs in academic institutions which have met the set criteria [CAEIAE 2005].

There are currently 37 universities in the United States that meet the standards required for recognition as CAEIAE [Fundaburk 2004]. Employers can then assess the capability of individuals based on the course they have completed [APEC 2004]. However, Fundaburk indicates that skills and attributes taught in the curriculum of these Centers for Academic Excellence had "no association with the skills and attributes employed, or addressed, by information systems security professionals in an information systems security work environment" with the exception of Applications and Systems Development Security [Fundaburk 2004].

Hum Kim, Deputy Director for Policy and Strategic Initiatives at the Department of Homeland Security's National Cyber Security Division, has stated that, "The Department of Homeland Security will encourage efforts that are needed to build foundations for the development of security certification programs that will be broadly accepted by the public and private sectors." The National Security Agency (NSA) had special extensions developed for existing certifications, including the CISSP Information Systems Security Engineering Professional (CISSP-ISSEP) specialisation [Norris 2004].

The CISSP is a prerequisite for obtaining the Information Systems Security Engineering Professional (CISSP-ISSEP) developed jointly between (ISC)^2 and the US NSA. (ISC)^2 has also developed the Certification and Accreditation Professional (CAP) credential in conjunction with the US Department of State. This credential is required for State Department employees who perform certification and accreditation functions within the Department [Williamson, (ISC)^2 2005].

2.4.3 United Kingdom

An independent study on the information security consulting industry provided for the UK Department of Trade and Industry in 2002 highlighted issues surrounding practices and qualifications in the industry. The Report's findings included that due to the complexity and rate of change in the knowledge base required for the industry, "the concept of information security as a chartered profession is probably not yet relevant" [Sundt 2002].

With regard to qualifications, the Report found that current qualifications or accreditations were "not considered as helping the information security services procurement process". Comments were made on the variable value of available qualifications, with those sponsored by professional bodies generally held in higher esteem than commercially motivated qualifications. Academic level qualifications were also generally held in high regard [Sundt 2002].

At the UK government level, the CESG Listed Adviser Scheme (CLAS) and the associated Infosec Training Paths & Competencies (ITPC) Scheme oversees the practicing of information security, primarily in government, by providing professional membership and qualifications. CLAS meets CESG's very specific information security authority needs. The four variants of the ITPC-administered Certificate of Infosec Competency awards are designed to certify people from different levels of an organisation that implement UK government information security policy and best practices [ITPC 2005].

The Institute of Internal Auditors (IIA) of UK and Ireland, a professional body, offers a Qualification in Computer Auditing (QiCA). The QiCA is specifically for the UK and Ireland and the Institute does not offer a globally available alternative to the QiCA.

The Information Security Professionals Working Group (ISPWG) report on *The Institute for Information Security Professionals* released in 2004 outlines a vision for a UK professional body for information security, much in the same manner as other chartered professions including engineers and accountants. An *Institute for Information Security Practitioners* would "provide Government and industry with highly professional practitioners in the field of information security, by providing a vehicle for members to demonstrate levels of judgment, skill and competence in front of their own companies, peers and clients" [ISPWG 2004].

At this stage, the field of information security certification is considered too young to allow for meaningful comparisons of the success of these countries' respective approaches. As such, this information is best used to acknowledge the identification of the issue at an international level, and the range of approaches being taken to move it forward.

3. THE CURRENT STATE

The current selection of information security skills accreditations available in Australia includes professional certifications and academic degrees covering a range of knowledge bases, from broad-based vendor-neutral certifications to vendor-specific and product-specific offerings.

The review of the current state of play in information security skills accreditation in Australia incorporates information on the range of available qualifications, along with their consideration or positioning with respect to three key certifiable elements:

- Knowledge
- Experience
- Trustworthiness.

From the perspective of information security professionals, it is widely accepted that marketability is the main driver for obtaining accreditation – the ability to gain access to positions that would not otherwise be available without such a demonstration of competence.

3.1 AVAILABLE QUALIFICATIONS

3.1.1 Academic Programs

A number of Australian universities offer postgraduate degrees in information security. Most of the postgraduate courses offered are Masters Degrees with Graduate Certificate and Graduate Diploma exit points. These courses extend for a period of one to three years on a part-time workload, depending on the level of the degree or diploma. Fees are often substantially higher than industry certifications; however, the Government does provide a fee assistance program for local students. Perth's Murdoch University offers an undergraduate Bachelor of Science in Internetworking and Security.

A report tabled by the US PITAC (Presidential Information Technology Advisory Committee) found that individuals providing and writing courses for universities may themselves be insufficiently qualified or knowledgeable. Some stakeholders in Australia hold the view that is arguable point whether universities can train, certify or accredit at a better quality than industry bodies.

University providers, see great value in their qualifications, crediting their longevity and their capacity for teaching students the ability to learn. One end-user of such skills indicated that he holds tertiary IT qualifications in high regard. One tertiary provider noted that industry certified professionals had sought university qualifications because they believed they did not learn enough from passing an industry certification and required further knowledge development. University programs attempt to give more industrial relevance to the material covered by examining case studies and having guest industry lectures.

While academic qualifications in information security are well regarded by industry, it has been pointed out that most current IT security practitioners are unlikely to be willing to return to academia to obtain a qualification.

3.1.2 Industry Programs

Judging by membership figures, the most popular broad-based certifications are internationally recognised qualifications such as the Certified Information System Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

At the time of writing this Report, there were 40,000 holders of the CISSP certification in 110 countries, with 600 of these based in Australia. CISA and CISM have a global base of approximately 38,000 and 5,000 certified professionals respectively. In Australia, 76 professionals are certified with CISM, and within Oceania, there are 680 CISA certified IT professionals. GIAC has 8,266 certified professionals internationally across a range of certifications. The number of GIAC certified professionals based in Australia was not able to be determined. In discussion with stakeholders, certifications such as those provided by SANS, ISACA and (ISC)^2 were generally well regarded.

The International Systems Security Professional Certification Scheme (ISSPCS) is a new international certification scheme developed in Australia by the University of Queensland, Electronic Warfare Associates (EWA) and the Australian Computer Emergency Response Team (AusCERT). The first class of professionals sat for the ISSPCS examination at the AusCERT Asia Pacific Information Technology Security Conference in May 2005. The ISSPCS certification is overseen by the International Systems Security Engineering Association (ISSEA) which has hopes that the certification will offer "an international and professional IT and Systems Security Certification Scheme that has wide credibility, jurisdiction and is genuinely international" [ISSPCS 2005]. Although developed in Australia, the ISSPCS scheme is intended to be international in nature and does not focus on the Australian marketplace. Currently more than 150 people have been granted ISSPCS Practitioner level certification or are in the process of being certified via the grandfathering mechanism.

In Australia, information security professionals who wish to complete a defined set of information security assessments for the Federal Government are required to attain the I-RAP certification developed by the Defence Signals Directorate (DSD) and SAI Global. The I-RAP program currently has 34 members. I-RAP is a purely Australian certification program and it cannot be recognised internationally.

A second certification program focused on the Australian market is the ISIG Professional Membership level. In order to achieve this recognition, an information security professional must be a member of ISIG, and must meet the following requirements. Professionals are required to attain at least one of the following certifications: CISSP, CISM, CISA or I-RAP for eligibility. As part of the application process, professionals must provide evidence of work experience directly related to information security. Professionals must provide information such as employer details, positions held, duration of the role and the security duties and responsibilities assigned to the professional in that time. The onus is on the professional to demonstrate four years of security-related experience, of which one year must be in Australia. ISIG Professional Members are bound by the ISIG Code of Ethics which includes standards of conduct regarding honesty, legal compliance, competence and diligence, professional development and integrity. ISIG currently has 12 members at the Professional Membership level, out of approximately 50 members. The Professional Membership status must be renewed annually.

In addition to the aforementioned industry and Government-supported certification schemes, are the vendor and product-specific certifications, such as Microsoft's Certified Systems Engineer (MCSE) – Security, and Cisco's Certified Security Professional (CCSP). Information security professionals can obtain training for these certificates through a wide range of third party training providers or can study for these certification exams independently. Vendor certification examinations can generally be completed at national testing centres on an on-demand basis. Vendors providing these courses were contacted for this project however the number of professionals holding each of the vendor certifications could not be determined.

These industry supported certification programs were well regarded by the majority of participants. For example, one consumer organisation indicated that all information security staff in their organisation should hold or be working towards the CISSP certification. They believed the broad-based CISSP satisfied 80 per cent of their organisation's requirements. The remaining 20 per cent was achieved through internal and self-learning, which were actively encouraged by the organisation. The content of the CISM program was also viewed favourably.

3.1.3 Standards

ISO/IEC 17024-2004: Conformity Assessment – General requirements for bodies operating certification of persons is an international standard developed with the objective of "achieving and promoting a globally accepted benchmark for organisations operating certification bodies" [SA 2004]. ISO/IEC 17024 states that a certification scheme should only be developed in response to specific government requirements or to a demonstrated market need or desire. The scope of the standard identifies requirements for a certification body, including the development and maintenance of a certification scheme for individuals.

The ISO/IEC 17024 standard is used as a method of measure for certifications in a number of industry sectors. Certification bodies have been accredited under ISO/IEC 17024 for certifying personnel and organisations against tasks such as Information Security Management Systems (ISMS) auditing, project management training, and product inspection and testing. In the USA, organisations such as the Board of Safety Professionals, the National Board for Certification in Occupational Therapy, and National Inspection Testing Certification Corporation are accredited with ISO/IEC 17024 [ANSI 2004a]. In the UK, organisations such as the British Institute of Non-Destructive Testing, and the European Registration Scheme for Personnel Competence are accredited with ISO/IEC 17024 [UKAS 2005]. As of April 2005, JAS-ANZ, a joint accreditation body for Australia and New Zealand, required all certification bodies under its scheme to comply with ISO/IEC 17024.

The ISO/IEC 17024 standard regulates the operation of certification bodies in three ways. Firstly, the standard dictates the criteria for policies and procedures of a certification body. Policies and procedures must observe fairness and equity among candidates; compliance to applicable regulations and statutory requirements; and the requirement for handling the resolution of appeals and complaints from the public. Secondly, ISO/IEC 17024 defines the structure of a certification body in order to ensure confidence in its competence, impartiality and integrity. Thirdly, a committee is required to take responsibility for the development and maintenance of the certification scheme. The certification body must prove it has the necessary financial resources for operation of the certification system and ability to cover related liabilities.

Other areas addressed by the ISO/IEC 17024 standard include the requirements for:

- 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.

The ISO/IEC 17024 standard also recommends a job analysis be conducted at least every five years to ensure that the certification scheme is still relevant to the role it certifies [SA 2004].

In June 2004, the American National Standards Institute (ANSI) accredited the CISSP certification offered by (ISC)^2 with ISO/IEC 17024 [ANSI 2004a]. In December 2004, the Information Systems Audit and Control Association (ISACA) applied to ANSI for ISO/IEC 17024 accreditation of their CISA and CISM certifications, with this accreditation granted in September 2005.

ISSPCS has also indicated that it is pursuing accreditation to this standard for its information security skills certification program. (ISC)^2 has indicated that they will be pursuing ISO 17024 accreditation for a number of additional certification programs. ISSPCS noted that the use of these ISO standards will assist in achieving convergence of standards in this area. It is expected that this will then allow for a clearer differentiation based on content.

3.1.4 Certification Fees

Completing international certifications can be costly for Australian information security professionals. This is largely due to high examination fees, followed by the requirement to re-certify at an additional cost after a period of time. In addition to the cost of the exam itself, most certifications do not include training or materials as part of the certification fee. The following is a brief breakdown of costs for the most widely recognised certificates in industry.

Interviewed organisations seemed most familiar with the CISSP certification offered by (ISC)^2. The standard cost for professionals wishing to complete CISSP certification is USD$599. A discounted price of USD$499 is offered to professionals who register for the examination 16 days prior to the exam date. An annual maintenance fee of USD$85 is required.

ISACA offers two of the more recognised certificates in industry, CISA and CISM. The CISA certification is priced at USD$460. The cost of the CISM certification is USD$455. The annual maintenance fee for CISA and CISM is the same. Certified ISACA members are required to pay an annual maintenance fee of USD$40, while certified non-members are required to pay USD$60.

The GIAC certificates offered by SANS have two distinguishable classifications, GIAC Silver and GIAC Gold. The GIAC Silver certificate is the first step for candidates applying for certification. Fees for GIAC Silver certificates range from USD$100 to USD$800, depending on the examination topic. Professionals are given the option of completing a GIAC Gold certificate 18 months after attaining the GIAC Silver certificate. The application fee for a GIAC

Gold Certificate is USD$200. Depending on the certificate, re-certification is required every two to four years.

The ISSPCS Practitioner level certification, developed by Queensland University of Technology, AusCERT and Electronic Warfare Associates, has an examination fee of AUD$500 plus taxes. Certification for the Practitioner level is valid for three years and re-certification is AUD$300 plus taxes.

The I-RAP program is a mandatory qualification for professionals who wish to complete specific security work for the Commonwealth. The application fee for I-RAP is AUD$275. Registration for the I-RAP program costs AUD$2,200, and is followed by a mandatory training and assessment fee of AUD$3,300. A maintenance training and assessment fee of AUD$1,650 is required annually. A discount of 10 per cent off the standard price is offered to members of AITSF.

Lastly, of the certifications examined, the least expensive qualifications are the vendor and product-specific certifications. Prices for vendor certifications range from AUD$180 to approximately AUD$250. These include certifications from vendors such as CISCO, Microsoft, Symantec and RSA.

Another choice available to Australian professionals is tertiary education. Australian students at tertiary institutions have the advantage of receiving Government subsidies; however, due to the duration of these programs and the inclusion of an 'education' component on top of a 'certification' component, the costs tend to be significantly higher. The following is a brief breakdown of costs for courses offered by educational institutions in Australia.

TAFE NSW offers an Advanced Diploma of Information Technology, specialising in e-security. The cost for the Advanced Diploma is AUD$1,995. This course is available in New South Wales, Victoria, and South Australia. The usual time of completion for this course is two years and six months full-time.

RMIT University in Melbourne has a postgraduate degree in information security. The program is divided into three stages, Graduate Certificate, Graduate Diploma, and Masters of Applied Science. The Masters is an incorporation of the Graduate Certificate and the Graduate Diploma. The 2005 fees are AUD$4,800 for each stage of the program. The course is completed over a period of one-and-a-half years full-time or three years part-time.

The Queensland University of Technology offers a Graduate Certificate in Information Technology, specialising in information security. The fees per credit point quoted for 2005 are AUD$100. A total of 48 credit points is expected for completion of the course, giving a fee for the course of $4,800. Based on the completion of two units per semester, the course can be completed in the space of 26 weeks.

Charles Sturt University offers a Masters of Information Systems Security over distance education. The cost of this degree is AUD$2,100 per eight-point subject. Students are expected to complete 96 points over the period of the course. Provided two subjects are taken per trimester, students are expected to complete the course in two years.

The importance of ensuring the cost effectiveness of any new Australian scheme was identified by many industry groups during the interview process.

3.2 KNOWLEDGE

3.2.1 Body of Knowledge

Over the years, various organisations have developed independent bodies of knowledge for information security certification. As a result, there are now a number of bodies of knowledge in direct competition with each other. The following is a brief explanation of the international bodies of knowledge studied by professionals undergoing various certifications.

The CISSP certification scheme is based on the Common Body of Knowledge (CBK). The CBK is a compilation of material for information security professionals and comprises 10 security domains. These 10 domains are:

- Access Control Systems and Methodology;
- Applications and Systems Development;
- Business Continuity Planning;
- Cryptography;
- Law, Investigation and Ethics;
- Operations Security;
- Physical Security;
- Security Architecture and Models;
- Security Management Practices; and
- Telecommunications, Network and Internet Security. [(ISC)^2 2005a]

The CISA certification scheme is based on seven areas of knowledge and application. These areas are:

- IS Audit Process;
- Management, Planning and Organisation of IS;
- Technical Infrastructure and Operational Practices;
- Protection of Information Assets;
- Disaster Recovery and Business Continuity;
- Business Application System Development; and
- Business Process Evaluation and Risk Management. [ISACA 2005a]

The CISM body of knowledge is based on five job practice areas, defined from a job practice analysis exercise intended to tie the material closely to the requirements of a practical information security management role. These areas are:

- Information Security Governance;
- Risk Management;
- Information Security Program Management;
- Information Security Management; and
- Response Management [ISACA 2005b].

ISO/IEC 17799 is commonly confused as a certification available for individuals but it must be noted that ISO/IEC 17799 certification is only applicable to organisations.

At an international standard level, ISO/IEC 17799 has a body of knowledge comprising these areas:

- Security Policy;
- Organisational Security;
- Asset Classification and Control;
- Personnel Security;
- Physical and Environmental Security;
- Communications and Operations Management;
- Access Control;
- System Development and Maintenance;
- Business Continuity Management; and
- Compliance [SA 2001].

The Colloquium for Information Systems Security Education (CISSE) is an American association established to serve as a "living body to bring government, industry and academia together" in supporting the education of information security professionals [CISSE 2005]. CISSE's predecessor, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) provides a body of knowledge in the standard for Information Systems Security Professionals, NSTISSI 4011. The body of knowledge for NSTISSI 4011 covers areas such as:

- Communications Basics;
- Automated Information Systems Basics;
- Security Basics;
- NSTISS Basics;
- System Operating Environment;
- NSTISS Planning and Management; and
- NSTISS Policies and Procedures.

The ISSPCS Practitioner certification scheme encompasses a Theoretical and Practical Knowledge Base (TPKB). The ISSPCS TPKB examines professionals on Security Processes in relation to specific fields of application, called Functional Disciplines. The eight Security Processes identified are:

- Strategic Security Management;
- Compliance (Standards and Legal);
- Asset Identification, Classification and Valuation;
- Security Risk Analysis and Assessment;
- Security Risk Treatment;
- Operational Security Management; and
- Security Operations for both Normal and Abnormal Conditions.

The six Functional Disciplines identified are:

- Fundamental Theory;
- Environmental and Infrastructure Security;

- Systems Security;
- Communications and Network Security;
- Physical Security; and
- Personnel Security. [ISSPCS 2005]

Given the brief examples mentioned above, the overlap within the areas defined by the various bodies of knowledge is apparent. However, there has been little work done to align the certifications and standards in a comprehensive and meaningful skills framework. At present, there are no in-depth skills measurements of existing certifications in the international marketplace.

In June 2003, ISIG prepared a mapping of the CISSP and CISA certifications against the ISO/IEC 17799 international standard. In the two years since this was completed, however, the content for the CISSP certification has been revised to remove US-specific content, and ISO/IEC 17799 is to be re-issued in 2005 with a new structure, resulting in the mapping no longer being current. To support further development in this area, SIFT has provided initial mappings of the CISSP, CISM, CISA and ISSPCS Practitioner bodies of knowledge against ISO/IEC 17799 in Appendix C to this Report.

3.2.1.1 Regionalisation

There is considerable debate about the amount, and level of Australian specific content that needs to be developed and offered by the various certification providers. The consensus is however, that there is no need for a national scheme to serve this purpose.

The ISSPCS (Queensland University of Technology) academic board contends that the current bodies of knowledge are too US-centric and have insufficient relevance for professionals in Australia and other regions including Asia and Europe. Others disagree with this assessment, noting that the Law, Investigation and Ethics domain of the CISSP's Common Body of Knowledge (CBK) is only one of 10 areas and the one with the least content.

ISACA has indicated that the CISM certification is an international program and it does not purport to offer any local or regional specific units. ISACA notes that while it could consider an Australian supplement for its certifications, it would need to ensure that equality was maintained between regions. Its view was that industry should not have a hierarchy of regions where the same certifications are ranked according to country of issue.

ISACA questions the need to regionalise, suggesting that the industry is heading towards global standards. (ISC)^2 has noted that its members have not indicated a requirement to have an Australian IT security skills certification to demonstrate local knowledge. As the marketability of certifications needs to be global an Australian certification would defeat that purpose.

A consumer/employer organisation noted that while the Australian technology experience is identical to overseas experiences, the business and regulatory environments are very different and experience in these areas is essential for good security execution in its sector.

Stephen Northcutt, Director SANS and GIAC, indicated that he believes Australian components for international accreditation schemes are an important concept, and this is already being implemented within SANS with the MGT 512 courses run in Australia including Australian legal components.

The ISIG Professional Membership category currently provides for regionalisation by requiring at least one year of experience in the Australian information security market to be eligible. The ISSPCS program was developed with the intent of meeting regionalisation needs but as the program is new, regional components have not yet been developed.

From a law enforcement perspective, the Australian High Tech Crime Centre noted that vendor and technology-specific qualifications, such as various RedHat, Microsoft and Macintosh certifications, are valuable as these qualifications are recognised in court. As these international qualifications are recognised in Australian courts, there is no real need for a new accreditation scheme to serve this purpose.

One participant indicated that there is no single international qualification that can be relied upon on which to base an 'Australianised' component.

The issue of regionalisation is dealt with in more detail in section 4.3 of this report.

3.2.1.2 Stratification

All participants agreed that information security is an extremely broad discipline and it is therefore not surprising that a number of certifications are now available in niche subject areas, nor that broad certifications are moving towards specialisations. Examples of the former include CISA (IS auditing) and GCFW (Firewall Analyst), and of the latter are the CISSP:ISSAP (Architecture) and CISSP:ISSEP (Engineering).

Members of (ISC)^2 have suggested extensions to the current range of certifications and consequently there have been moves to certify additional in-depth competencies beyond the baseline credential. (ISC)^2 has identified a need for additional competencies in areas such as forensics, critical infrastructure protection, privacy, governance, risk management and compliance.

While these specialisations are content-based, an alternative approach is for certifications to be separated by 'seniority.' The ISSPCS certification scheme has proposed four levels, with the first and only currently available level being the ISSPCS *Practitioner*. This entry level is available to all ISSPCS applicants. The remaining three levels of ISSPSC certification are *Professional*, *Mentor*, and *Fellow*. Progression to each level is dependant on successful completion of the previous level. It is understood that higher certification levels require a greater involvement in the information security industry, along with an additional exam and experience requirements as yet to be determined.

ISIG, while supporting CISSP, CISA and CISM, recognises that current certifications are struggling to keep up with the explosion in sub-disciplines within the industry. SANS acknowledges that CISSP and GIAC certifications meet some but not all of the industry's needs. SANS is aware that there are many skills that current accreditations do not cover and it is working to address this.

One consumer/employer organisation suggested that while there currently existed a great deal of knowledge and experience at the desktop this knowledge and experience diminished along the hardware chain with mainframe expertise difficult to obtain.

Another provider indicated that students with management experience have attended their programs to enhance their technical knowledge, particularly in cryptography and Public Key Infrastructure (PKI).

ISACA believes that management is far more relevant for a certification because of the persistent nature of these skills. Therefore ISACA does not see a need to segment a certification like CISM into different specialisations.

On the other hand, SAI Global believes there is a lack of management principles taught in the current certification programs, suggesting that individuals in the industry generally come from technical and network security backgrounds and lack an overall management perspective. TAFE NSW has identified that there is poor alignment of technology with business objectives in current programs and a lack of appreciation for business concepts.

One consumer/employer organisation identified a problem that managers were using broad-based certifications to determine employee competence where specific niche skills were required. In contrast, another consumer/employer organisation indicated that it placed little emphasis on vendor (narrow) qualifications when recruiting information security professionals, finding that individuals with a broad exposure to the information security body of knowledge were more desirable.

The industry is divided on the need for management level information security certification, and the required content to provide an understanding of information security management concepts in the existing certification programs. There is a greater degree of agreement regarding the merits of both broad and narrow based information security certifications, with the specific requirement depending on the organisation and requirements of the role. It is expected that specialisations will be developed by certification vendors based on market demand and will succeed where industry acknowledges the need and value.

3.2.2 Assessment

The majority of the industry certification programs assess knowledge through an examination conducted in person in university-level exam conditions.

CISSP examines professionals in all 10 security areas of the CBK in a six-hour examination consisting of 250 multiple-choice questions. For CISA candidates must complete 200 multiple-choice questions regarding the seven areas within the body of knowledge, in four hours. For CISM, a similar requirement of 200 multiple-choice questions in relation to the five job practice areas applies, again over four hours. Candidates completing the ISSPCS Practitioner certification are required to sit a four-hour examination. The I-RAP certification scheme has a mandatory two-day training program and a written exam.

A common criticism of existing certification programs requiring an exam-only assessment is the failure of this method in validating the ability of individuals to practically apply knowledge. Professor Bill Caelli, Head of the new School of Software Engineering and Data Communications in the Faculty of Information Technology at the Queensland University of Technology, has commented on the inadequacy of industry certifications in testing the competency of individuals and the ability to apply this in a real-world situation [Gray 2003].

The I-RAP program structure allows for an effective assessment of individual competence with respect to the specific I-RAP audit tasks. The standards against which competence is assessed are well known and structured, and as such it is easy to test the skills held by applicants. I-RAP assessors use predefined checklists for completing audit tasks and these checklists are returned to DSD upon completion. As a result, the DSD can complete an

effective closed-loop assessment of competence, including a verification of the candidate's ability to apply the theory in a real-world audit scenario.

AusCERT and ISSPCS's Academic Board indicate that evidence of continuing involvement in the industry would be a good indicator of competence as there is a process of natural selection. They noted that while a quantitative exam is the primary requirement at the Practitioner level, higher levels will require mainly qualitative assessments.

A view was expressed by one participant that intensive short courses for certifications greatly devalued these certifications with the net effect being that candidates holding a similar level of certification have distinctly different underlying skill levels. While university courses are expected to produce a more rounded and broadly applicable skill set, it may not be possible for consumers of such services to distinguish between the two certified professionals.

ISSPCS indicated that there is a 'Teaching Education Development Institute' at the University of Queensland which focuses on how individuals are assessed. The ISSPCS development team has made extensive use of this group to ensure the exam approach and format accurately assesses an individual's practical competence. Similarly, ISACA has a number of groups that operate to ensure the ongoing standards of the program, including the Test Enhancement Committee, the Certification Board and ISACA Governance. Certification decisions are subjected to Board review on an annual basis to ensure close monitoring and improvement of the process. $(ISC)^2$ has a committee dedicated to the CBK from which the $(ISC)^2$ credentials are drawn, along with a Test Development Committee responsible for all exam-related certification materials.

3.2.3 Continuing Professional Education (CPE)

At present, all the main industry certification schemes in place in the Australian market require some degree of continuing professional education, which contrasts with the majority of academic programs which grant degrees and diplomas which do not have an ongoing requirement.

Consumer/employer organisations commented on the importance of up-to-date and relevant knowledge.

The value of CPE as currently implemented was questioned by a number of participants who suggested that the CPE approach generally allows the certified individual to choose whether they want to undertake an ongoing education or simply meet minimum ongoing certification requirements. ISACA and $(ISC)^2$ conduct periodic audit checks to verify experience and claims of CPE points, however these checks cover the range of activities across which CPE points can be claimed, rather than the integrity of the process itself.

Under the GIAC program retesting is required to verify ongoing competence, but this is not a popular approach.

It was agreed that effectively managed ongoing professional development was a necessity for any Australian information security skills accreditation program.

Given the broad agreement on the importance of continuing professional development and ensuring professionals maintain a suitable level of knowledge, alternatives to the existing approaches to CPE and re-assessment need to be considered.

3.3 TRUSTWORTHINESS

3.3.1 Trustworthiness and Professional Ethics

Many organisations have identified trustworthiness as the most important issue to consider for a scheme, although it is acknowledged that trustworthiness is difficult to certify.

It was agreed that ultimately, staff trustworthiness checking has to be the responsibility of the employer through due diligence, although it can be especially challenging for small to medium sized organisations to gauge trustworthiness. Police checks are often inadequate in determining the trustworthiness of a security professional; with an individual's trustworthiness judged only to the extent to which claims of previous experience are verifiable. It is however difficult to verify 'experience' since most organisations will only state the duration of employment and their rules do not allow them to report dismissal reasons. While it is recognised that the due diligence process has high associated costs there is a necessary and unavoidable level of due diligence required of a company's management or human resources personnel in verifying experience.

The (ISC)^2, ISACA and ISSPCS have codes of conduct and ethics that their certified professionals are required to follow, however the related complaint mechanisms are not well known and issues with certified professionals are often not reported.

ACS is working with CPA Australia and Engineers Australia to jointly accredit software engineers, with these professional groups having the authority to revoke certifications. ACS has identified that in the information security space, voids are often filled by engineering and accounting professionals, therefore the involvement of these groups is essential.

3.3.2 Professional Liability

The Professional Standards Council (PSC) allows professional bodies to apply for a scheme to cap the liability of its members. In return, the bodies are required to have systems in place to regulate their members. With respect to an accreditation, the system must be able to identify and administer suitable accreditations within the professional body.

Each year, the professional body is required to report to the PSC on the strategy components and key performance indicators of the system. Under the PSC scheme, professional bodies must have insurance and liability disclosure. There is no direct contact between the PSC and the professional body's members – it is the professional body which acts as the regulator of its members.

The PSC scheme is created under the *Professional Standards Act 1994 (NSW*) and the *Professional Standards Act 1997 (WA)* and as such the relevant schemes are currently only available within these jurisdictions. Most other Australian States and Territories are currently progressing legislation and programs to establish similar schemes with a view to achieving national coverage.

Within this context, the ACS has proposed a two-tiered system for ICT professional accreditation:

- Using the Professional Standards Council program, the first tier will be a Certified ICT Professional accreditation, intended for consultants. These can have

specialist areas including security. To be a CICTP it will be necessary to provide insurance details with this being subject to audit;

- The second tier is a Practising ICT Professional, which does not require professional indemnity insurance. However, it does require referees to gain entry to this tier and an annual activity statement to verify CPE.

AITSF notes that while the PSC scheme may be useful in supporting smaller organisations, liability provisions in contracts generally provide the structure around professional liability in the IT security industry.

3.4 EXPERIENCE

Many organisations noted in discussions that the information security field was relatively immature and as a result experience in this field is not yet a reliable indicator of competence. In a field where demand for professionals outstrips supply, individuals are obtaining 'credible' experience to attempt to demonstrate their capabilities but as participants noted time spent in a position does not of itself demonstrate relevant capabilities.

Almost all of the certification schemes available to Australia require professionals to fulfil a set of prerequisites before their application is accepted. A sample of the entry points for the more common certifications completed by professionals follows:

- The CISSP certification requires a minimum of four years of professional experience in the information security field, or three years plus a college degree. Substitution for experience is allowed, with a Masters Degree in Information Security from a National Centre of Excellence replacing one year towards the four-year requirement.
- Professionals wishing to qualify for CISA certification must submit evidence of a minimum of five years of professional IS audit, control or security work experience to ISACA. The following exceptions are allowable:
  - A maximum of one year of IS audit, control or security work experience may be replaced by one full year of non-IS audit experience, or one full year of information systems experience, or an associate's degree.
  - Two years of IS security audit, control or security experience work may be replaced by a bachelor's degree.
  - One year of IS audit, control, or security experience may be replaced by two years experience as a full-time university instructor in a related field, such as computer science, accounting and IS auditing.
- The CISM certification requires professionals to have a minimum of five years' information security work experience, with a minimum of three years' information security management work experience in three or more of the job practice analysis areas. Substitution is also allowable.
- The ISSPCS certification requires professionals to have a minimum of three years' work experience in information security, or a three-year IT-related degree qualification. For grandfathering, a range of existing certifications can be used, such as a current CISSP, CISM, SANS GIAC GSE or an SSE-CMM Appraiser certification. Applications are assessed by the academic board and reference

checks are conducted. With the University of Queensland as a key body, academic qualifications are easily verified.

- RMIT University accepts undergraduates in a scientific field or equivalent in its master's course. However, substitution is allowed at the discretion of the program leader.
- Charles Sturt University is similar in its prerequisites, requiring an undergraduate degree or equivalent from students enrolling in its distance education course.
- Queensland University of Technology requires an approved bachelor's degree in IT from a recognised tertiary institution with a point average of at least 4.5 on a seven-point scale. QUT will also accept students who provide evidence of suitable qualifications through a Recognised Prior Learning process, and significant full-time IT work experience.
- TAFE NSW permits people who have completed Year 12 or equivalent to enrol in their Advanced Diploma course.

The prerequisites for vendor-specific certifications vary but most, such as Cisco, Symantec and RSA recommend before candidates apply for certification, but do not mandate, a minimum period of experience with relevant product packages.

Alternatively, ISIG offers Professional Membership for those who are qualified with either CISSP, CISM, CISA or I-RAP. Professional Members must have four years' work experience in an information security-related area, gained over the previous 10 years, with at least one of the four years in Australia. A university degree may be substituted for two years of experience, and a higher degree or Graduate Diploma in information security may be substituted for an additional one year of experience.

The pre-qualification requirements for joining I-RAP are:

i. Evidence of current CISA certification and evidence of a minimum one year of experience, gained within three years of the time of application, auditing information security systems; or
ii. Evidence of current CISSP certification and evidence of a minimum one year of experience, gained within three years of the time of application, auditing information security systems; or
iii. Evidence of appropriate academic qualifications relating to information technology, relevant to understanding information security systems and evidence of a minimum one year of experience, gained within three years of the time of application, auditing information security systems; or
iv. Evidence of a minimum two years' experience, gained within three years of the time of application, auditing information security systems.

A number of organisations have also noted that many quality information security professionals do not have degrees or certifications but have considerable experience. For these professionals, there is often a lack of interest in obtaining a certification. Several consumer/employer organisations indicated that qualifications are not a mandatory requirement for recruitment as prior recruits, without qualifications but with experience, have proved to be exceptional information security professionals.

Current ACS accreditations have a demonstrated equivalence process and a skills assessment process as additional entry points to their certification scheme. There is also a

'senior manager' pathway for people who have a demonstrated history of performance in the area. At present, to validate experience, ACS requires individuals to provide certified documentary evidence of their experience.

$(ISC)^2$ observes that judgment improves with carefully managed experience and that experience needs to extend beyond security skills to include general management, such as budgeting, people skills, and presentation skills.

Given the choice of similar Australian or foreign experience most recruiters agreed they would elect to employ the professional with Australian experience.

4 THE NEED

Participants were given the opportunity to respond to the project's investigation of the industry need for a new Australian information security skills accreditation. Discussions were allowed to range according to the interests and concerns of the participants and as such the issues identified were not pre-determined by the interview process.

The needs identified by stakeholders and industry participants fell broadly into four categories:

- the need for a mechanism to accurately assess competence;
- the need for information security professionals to possess greater knowledge;
- the need for professionals to possess knowledge and understanding specific to the Australian business environment; and
- the need for an informed market.

In order to discern the need for an Australian information security accreditation scheme, interview participants were asked what gaps existed in current accreditation schemes and whether the implementation of a new Australian accreditation would supplement an information security professional's knowledge, trustworthiness, experience and competence at an international level.

The need for Australia to have its own accreditation scheme was questioned, with the observation that an Australian information security skills accreditation could unnecessarily increase the prices for information security services.

ESecurity Australia members have indicated that there is currently no customer requirement for security professionals to be certified. They indicated that while they were content to obtain relevant certifications as individual practitioners, they did not believe that consumers/employers of information security services, particularly small organisations, required certified professionals. Members would not regard any requirement for certification of information security professionals as significant in the improvement of quality in service. Large employers have indicated to members of eSecurity Australia that certifications are "nice to have" rather than a "must have" requirement for being retained to complete a security job..

It was noted that Australia already has access to certifications that work for the industry. However, if there were to be a new accreditation scheme it was important members said that it be aligned with existing international standards to avoid creating a support structure. Industry already has reference books and study materials for current information security skills certification examinations. Any new Australian accreditation scheme could also devalue the international certifications of existing professionals.

Participants agreed that Australian information security skills needed to be accepted globally. Information security is an export industry, allowing and requiring professionals to work anywhere. As a result Australian professionals require global recognition for their skills and qualifications.

It was suggested by some participants that the need for a scheme is an issue that has a wider application across the whole of the IT industry, and there would be benefits in leaving the

issue until a fuller review could be completed at the IT professional level before accreditation for sub-specialisations should be addressed.

4.1 The Need for a Mechanism to Accurately Assess Competence

Many interview participants were interested in the role an Australian accreditation scheme could play in promoting the image of information security professionals. Participants recognised the need to regulate the industry and remove unreliable or untrustworthy practitioners.

It was seen as essential that employers rely on commercial good sense in assessing the competence of a professional i.e. technical interviews must be conducted with candidates if technical knowledge is required. Of more importance is obtaining references from past employers. Due diligence will always be essential.

The difficulty in judging the competence and trustworthiness of information security professionals based on their stated experience was recognised. Qualifications are valuable as they indicate a degree of base knowledge and certification programs measure a level of knowledge, establishing a benchmark for employers and interested third parties.

While large organisations generally have the experience, skills and current market knowledge to recruit appropriately, it is difficult for small to medium enterprises to identify professionals with the right skills.

While some participants indicated that accredited security professionals have to date served their clients well, others indicated that critical infrastructure operators do not believe current certifications are meeting their needs, as they do not sufficiently guarantee the knowledge or quality of an information security professional in a critical infrastructure environment. This is particularly the case for industry sectors forming part of Australia's critical infrastructure that have not traditionally been online, such as transport, freight forwarding and water provision.

It was suggested that there is a need to identify differences in the available bodies of knowledge to provide a mapping of skills covered by each certification. Since no licensing or certification process will stop or capture the 'cowboys' in the market, industry should investigate the possibility of expelling professionals from a certification scheme should they breach the codes of conduct and ethics.

One need identified by a critical infrastructure operator, was to ensure information security knowledge fields were readily distinguishable, to support greater clarity around required knowledge. For example, security practitioners, technical specialists and business continuity managers are all in slightly different fields all under the broad title of information security.

A participant highlighted the challenge of recruiting information security professionals who are skilled in the full range of technologies, new and old such as mainframes and Unix. They noted that current qualifications did not equip recruits fully for their information security roles. They believed that text books were not teaching these information security topics adequately and the theory of risk was not being translated into operational experience.

Other organisations did not enforce a requirement for a single certification in their recruitment process. Instead they first identified the skills required for a security role then sought the best

candidate, with some roles requiring vendor qualifications and others requiring business experience.

The observation was made that there were many skilled people in the market without degrees or certifications. One company emphasised the interview process to determine cultural fit, knowledge and experience and said it was more inclined to consider certifications for technical roles. This organisation said they would not place much emphasis on an Australian information security skills accreditation scheme.

These varied experiences highlight the differences in recruitment practices between organisations. Some organisations seek a single certification to provide a base level of knowledge, whereas others take a more active role in defining knowledge requirements for each specific position.

A representative from an information security and risk management-focused recruitment organisation said there had been little demand from clients for candidates with formal accreditation. Although certifications such as CISSP were regarded as a benchmark by practitioners in the industry, hands-on commercial experience was regarded as more important to clients. It has been suggested that as the security market matures, more clients will seek candidates with tertiary and professional accreditation as well as a level of experience. Recruiters indicated that where candidates have similar skills and experience, the deciding factor in the selection process would come down to qualifications.

Some organisations with specific needs have developed their own programs and initiatives, designing a scheme to test and endorse professionals for their work requirements.

A specific need in the market led to the development of the I-RAP program. The DSD had identified a series of upcoming government initiatives, such as FedLink, which were expected to increase the demand for DSD services. As such DSD anticipated the requirement for suitably qualified professionals and it designed the I-RAP program to test and endorse professionals for this work. The DSD requires these professionals to demonstrate their knowledge of government information security policy and the I-RAP policies and procedures.

Participants agreed that although there is an issue with assessing professional competence within the industry, a new Australian information security skills accreditation program would not necessarily provide an ideal solution to the problem. Many agreed that current certifications already have established a benchmark and an indication of base knowledge. Similarly, many participants emphasised the importance of the interview process as an appropriate mechanism for assessing competence, rather than relying purely on professional certification.

4.2 THE NEED FOR INFORMATION SECURITY PROFESSIONALS TO POSSESS GREATER KNOWLEDGE

In order to discern whether an Australian accreditation is required to fill the gaps in knowledge of existing certifications, participants were asked to comment on how comprehensive current certifications are in their coverage and examination of information security skills and knowledge, and whether certified professionals possess the appropriate skills and knowledge to complete assigned tasks.

Many participants indicated that there was no need to change the current approach to vendor and product-specific certifications, and that in these particular areas professionals have been found to have the necessary skills to complete required tasks.

Others suggested that each role will have a required level of skills, experience and knowledge and that the level of required knowledge should be defined and assessed as a part of standard recruitment procedures. Organisations relied on different qualifications depending on the role; for example, recruiting a broad-based qualified professional, such as CISSP, for security management roles, and professionals with technical certifications for technical roles.

Some participants believed that there was a need for an ISO standards-based accreditation model beyond overseas certifications such as CISSP and CISM.

Members of eSecurity Australia have faced challenges with the I-RAP program. According to members of eSecurity Australia, I-RAP is regarded as too costly by some members to undertake and some members feel that similar levels of systems audit skills could be evidenced by an ISACA international systems audit certification. However as noted in the previous section of this report, the I-RAP program was designed to specifically incorporate elements of government information security policy, rather than an attempt to create a competitor to the existing certifications. As such, a comparison between I-RAP and international certifications is only partially valid.

On the other hand, some experienced challenges with using existing certifications which did not provide a broad education. One difficulty was the recruitment of professionals who have the ability to develop business information security policies as well as a suitable technical background to understand the broader implications of policy issues.

In recognition of the changing needs of industry, ISACA evolved from a pure information security (IS) audit organisation into an association covering IS audit, IT governance and security. ISACA recently formed an alliance with ASIS and ISSA to help organisations recognise the growing need for training in the Chief Security Officer (CSO) and Chief Information Security Officer (CISO) roles. $(ISC)^2$ has similarly created a 'road map' for the development of information security professionals into CISOs.

$(ISC)^2$ has said that information security workers who do not seek to obtain and maintain professional status and competency are likely to remain under-skilled. Likewise, those who may obtain certification within schemes that do not require continuing professional education (CPE) are likely to become outdated in their skills.

SANS similarly asserts that the biggest problem is currency with information security professionals remaining under-skilled despite having qualifications. SANS does not believe that the continual learning approach to certification is effective. SANS gives the example of GIAC re-testing, which is not popular among members, as an alternative.

Most participants currently use certification as a means to determine the level of base knowledge acquired by a professional. The issue does not seem to be the lack of essential knowledge and skills taught by current certifications; in the rapid-paced information security environment, participants were more concerned with the relevance and currency of information security information taught by certifications. There was a need expressed for certification bodies to maintain the relevance of certifications, together with a need for information security professionals to pursue continual career development. The skill observed as lacking with most information security professionals, regardless of certification, was the

ability to understand both the business and the technical requirements of information security, and developing security controls appropriately.

4.3 The Need for Professionals to Possess Knowledge and Understanding Specific to the Australian Business Market

Interview participants were asked whether Australia needs its own accreditation to compensate for cultural and/or content differences between Australia and other countries. The majority response was that although there are regulatory and legislative differences between Australia and other countries, that there is no need to create an accreditation scheme unique to Australia. Participants also raised the issue of global limitation if Australia sought to develop its own scheme.

Where a regionalised certification approach has been suggested, elements identified as being region-specific include:

- Legal and regulatory environment.
- Government standards such as ACSI 33.
- Business environment and context.
- Cultural issues.
- Aligning technology with business objectives.
- Language.

Within government it was suggested that there is a need for professionals to have knowledge of the Protective Security Manual (PSM), ACSI 33, and AS 4360, and this knowledge is not covered by existing certification programs. There may be a need for a 'bridge' to capture the intricacies of the Australian environment over the top of international certification programs.

SANS members have indicated that professionals need to be able to demonstrate local knowledge and an Australian IT security skills accreditation scheme could be a means to do this. In other countries, demonstrating regionalisation is also an issue for professionals. $(ISC)^2$ has done 'regionalisation' work for the US Government, and is currently discussing arrangements with China, Canada, Singapore, the UK and a number of other countries.

Other participants indicated that the practical experience requirement of certifications was sufficient to ensure that a professional has the necessary work experience and had developed the necessary social skills and environmental understanding to fulfil tasks as an information security professional. For these requirements, Australian experience was no different from experience gained overseas.

Concerns were expressed that although offerings from international providers were technically correct, there was a need for an overarching accreditation scheme which incorporated Australia's legal and regulatory context. For example, while the CISSP does not make reference to Australian standards such as AS/NZS 7799 and AS/NZS 4360, the concepts are included.

There was a divergence of participant's opinion as to whether more than one standard for information security skills certification was viable, with some participants suggesting that I-RAP should be adapted into a broader Australian certification scheme and others contending that no single qualification could meet the breadth of industry need.

Participants were also divided on whether or not an Australian content was required. While some felt that it was important to have an understanding of the Australian environment, others maintained that the practice of security principles only differed slightly on an international scale. However, it should be acknowledged that the level of knowledge and understanding required of an information security professional is also dependent on the nature of the organisation and the role of the professional. For example, while it is important for a professional working in a Government agency to be aware of the PSM, or the ACSI 33 standard, it may be more relevant for a professional working in the telecommunications industry to understand implications of Australian telecommunications interception laws.

4.3.1 Requirement for local legal & regulatory knowledge

The requirement for information security professionals to have knowledge of the Australian legal and regulatory environment was an area subject to considerable discussion by participants. While there was an in-principle consensus that this knowledge is worthwhile, there was disagreement as to whether this should be a mandatory component of a certification program rather than merely an additional element of knowledge to be considered when selecting an information security professional.

One view expressed was that Information and Communications Technology (ICT) professionals needed to have a good understanding of the legal and regulatory environment in Australia. It was suggested that some overseas professionals cannot fit into the culture of Australian organisations as they have a different understanding of ethics and regulations. It was noted that the issue of regionalisation is also faced by other professions, such as the legal sector where of foreign lawyers are required to complete bridging courses before being allowed to practice in Australia.

Other participants acknowledged the need for professionals to understand privacy and surveillance laws in Australia, but saw it is an organisation's responsibility to educate their employees about boundaries. Participants believed that information security professionals should not be expected to know the legislative differences.

Some Australian ICT companies have had issues with legal compliance in the past; eg, providers of IT services might be operating appropriately according to US law but might be violating telecommunications interception laws in Australia. As legislation changes, there may be a need for a professional organisation to ensure continuing education in this area.

Both small business representatives and larger companies indicated that it is necessary for Australian information security personnel to understand the Australian legal and regulatory environment, however participants differed in their views as to who should provide this knowledge.

Some organisations have business units within the organisation responsible for ensuring regulatory compliance, but nonetheless would value information security professionals having knowledge of the telecommunications industry as well as Australian legal and regulatory knowledge.

The legal and regulatory knowledge required of professionals varied depending on the participant's industry sector. The majority of participants agreed that it was important for information security professionals to have an understanding and awareness of Australia's legal and regulatory environment in order to practise information security within legal

boundaries. However, participants did not view an Australian information security skills accreditation scheme as a solution to this problem.

4.3.2 Appropriateness of information security professionals providing legal & regulatory advice

In addition strong views were expressed by some groups as to the appropriateness of information security professionals providing legal and regulatory advice to their clients.

Participants agreed that although it was beneficial for an information security professional to have knowledge of legal and regulatory issues, organisations should not be turning to information security professionals for legal or regulatory advice.

4.3.3 Extent of required regionalisation

Participants were questioned on the extent to which current certifications should be regionalised to cater for information security professionals practising in Australia.

It was noted that many Australian companies are subsidiaries or parent companies of companies in the US, Europe or Asia, and the laws of those jurisdictions must be taken into account. International legal and regulatory frameworks are often relevant to Australia, with legislation such as Sarbanes-Oxley and the European Privacy Directive having an impact on Australian companies operating internationally. However, participants noted that legislation between states often differed, for example privacy legislation.

Providers advised that for regionalisation to be offered there needed to be clearly defined boundaries and jurisdictions within relevant regulatory regimes. Participants also observed that individual professionals shared part of an organisation's responsibility for compliance.

4.3.4 Maintaining international relevance

Participants questioned the validity and quality of its benefits on a global scale of an Australian information security skills accreditation program. Participants were concerned that Australia would be removing itself further from a field that increasingly required professionals to work on a global scale, regardless of geographic boundaries.

Standards Australia believes there is no need for a uniquely Australian scheme as it would require global recognition. It would also be necessary to ensure that any new scheme was not a restraints to trade. Standards Australia does accept the need for knowledge of Australian regulation and legislation in order for information security professionals to complete their responsibilities in the market, but deems it sufficient to have Australianised components extended from international accreditation schemes to cover this need.

It was considered important to have access to internationally recognised schemes with more frequent course offerings, and a greater recognition of the value of information security skills accreditation. The information security industry itself is heading towards global standards. Australian professionals require global acceptance and marketability on a global level.

(ISC)^2 agrees that in many instances a solid understanding of Australian regulation would be needed. Most likely it would also require international accreditation to meet the needs of increasingly internationalised commerce, due to the proliferation of multinational corporations and international cooperation among governments.

Consensus from participants was that an Australian information security skills accreditation program would be worthwhile only if it could achieve recognition and acceptance on an international level. The majority of participants at interview were satisfied with the current offerings of certifications recognised by organisations based in Australia, as these are internationally 'portable'.

4.4 THE NEED FOR AN INFORMED MARKET

4.4.1 Content & relevance of certifications

In order to determine if an Australian accreditation program is necessary to provide relevant information to professionals practising in Australia, participants were questioned on the adequacy of content and relevance of the certifications available to Australia.

The consensus was that for critical infrastructure operators a framework of accreditations is needed that match required skill needs. There are currently multiple certificates with different values available to an uninformed market. Industry needs a mechanism to understand what current certificates imply. From a consumer/employer's perspective the challenge is to understand what information security services they are buying. It was considered that Australia does not need to adapt existing programs or create new programs as there are already too many in existence.

There was a belief expressed that more work needed to be done to assist SMEs appreciate their need for information security. Non-technical business operators expect to employ IT staff or contract IT resources who have an understanding of their organisation's broad needs and security requirements. Many employers are ignorant of IT accreditations in general and are certainly unaware of accreditations for information security professionals. .

The major issue with the current qualifications noted by participants was not the lack of relevant content or knowledge; rather it was the lack of understanding by employers as to what the qualifications offered. Participants admitted difficulty in distinguishing the skills examined by the various qualifications and proposed that the mapping of skills to qualifications would be of more assistance than the creation of a new accreditation scheme.

4.4.2 Membership of programs

Industry groups and representatives also observed that it was difficult to distinguish if professionals were certified, and that certification did not necessarily equal quality or competence.

Since it is not commonly known who is certified and who is not, referees are very important. It was suggested that there should be more openness about who is certified and better use of certification providers' ethics and complaints processes to assure this.

While most international certifications have an enforced Code of Ethics mechanism, participants noted that it was unlikely that many people would report complaints back to $(ISC)^2$ and ISACA. ISIG has suggested localisation in this area to provide improved assurance.

It is expected that as information security skills accreditation awareness grows, there will be a similar growth in the use of these credentials by professionals to differentiate themselves. It is known that at least some of the certification providers have searchable online databases of

certified professionals, and increasing the awareness of these facilities is expected to support the verification of membership and willingness to report ethics breaches back to providers.

4.4.3 Due diligence requirements

Participants believed that there were common misunderstandings about an organisation's responsibility to due diligence when engaging any professional. A professional's achievement of certification should not be seen by organisations as a replacement for due diligence in the form of background checks and thorough interviews.

A need was identified to educate employers about what constitutes due diligence. It was proposed that consumers/employers of these professionals needed to clearly define their requirements in a concise manner identifying the set of skills and knowledge they expect information security professionals to possess.

There is no suggestion that this issue is unique to the information security industry. In all industries there is a need to ensure that a given candidate for a role is technically competent, possesses the required knowledge, will be a cultural fit, and has the necessary integrity for the position. Certification programs have a limited capacity to meet these requirements.

5 THE WAY FORWARD

On the 15 June 2005, a workshop with key stakeholders and interested parties in the information security industry was held to present the initial findings of SIFT Pty Ltd on the current state of information security skills accreditation in Australia and to provide a forum for discussion on the issues identified by the initial findings. The objective of the workshop was to identify an acceptable 'way forward' for the industry on the issue of information security skills accreditation in Australia. The workshop was structured into three presentations

- Report on the Current State,
- Report on the Need, and
- Models and Options.

Each presentation was followed by an open discussion with workshop participants. The following sections detail observations of workshop participants in relation to the findings presented by the consultants.

5.1 CONTEXT OF OPTIONS

5.1.1 Elements of a Successful Program

Workshop participants were presented with the following diagram which illustrated the key elements for achieving a functioning model for information security skills accreditation in Australia.

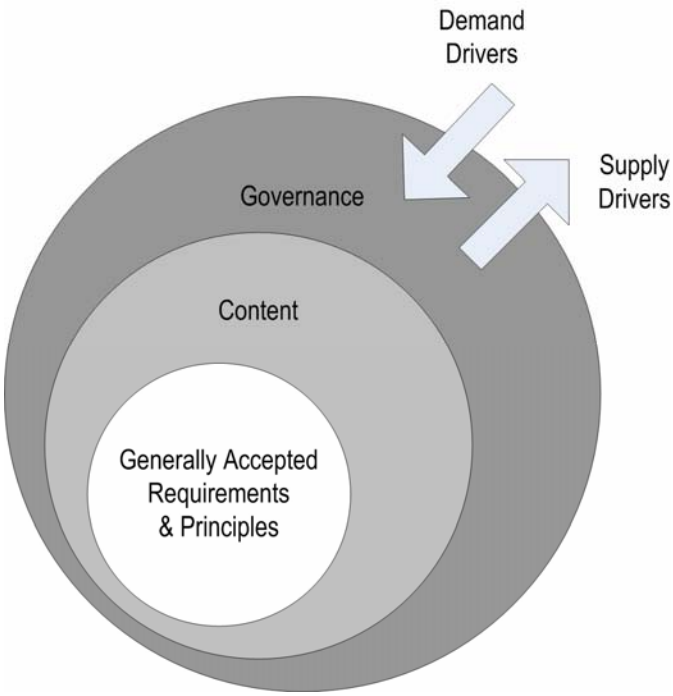


Figure 1: Elements of a successful accreditation program

Definitions of each of the broad elements are included below.

5.1.1.1 Generally accepted requirements & principles

A number of fundamental requirements were identified and remained consistent throughout discussions with a wide range of organisations including information security professional service providers, consumers, representative bodies, and end-users.

5.1.1.2 Content

Issues surrounding the contents of the body of knowledge required by an information or IT security professional, along with discussion on the need for specialisation and regionalisation of certifications were discussed.

5.1.1.3 Governance

In examining the governance aspects of a way forward, the full range of alternatives – from a laissez-faire market forces approach to a prescriptive licensing requirement were canvassed.

5.1.1.4 Demand and supply drivers

In order for any Australian scheme to succeed, it would be necessary to identify drivers and impediments to adoption both for providers and consumers/employers of information security professional services.

5.2 GENERALLY ACCEPTED PRINCIPLES

When discussing the way forward with stakeholders and interested parties in the initial phase of this project, a number of items were identified as requirements, principles, or 'boundaries' on approaches that would receive industry support. Workshop participants were presented with the following headings which sought to capture these principles and requirements.

5.2.1 Do not 're-invent the wheel'

The vast majority of organisations interviewed agreed that any Australian scheme should build on the work completed by existing certification programs rather than 're-inventing the wheel'.

Workshop participants agreed that industry should not look at creating a solution based on a new body of knowledge. The solution should build upon knowledge already available from current schemes.

5.2.2 Provide an open standard

Many industry professionals have already obtained well-recognised international certifications, and in order to maintain industry support, it was necessary to provide for these certifications to be recognised within any new information security skills accreditation scheme. Similarly, it was necessary to provide for industry certifications and academic qualifications to co-exist.

Workshop participants agreed that the agreed solution must be inclusive of programs already in existence, including existing certifications, along with tertiary education degrees and diplomas.

5.2.3 Minimise financial impediments

To ensure wide acceptance and use, any new scheme must provide value for money. This principle also extended to ensuring it was not necessary to join a large number of schemes to ensure 'coverage' of the information security skills arena.

Workshop participants agreed that the cost of developing and maintaining a solution should not create a barrier to the participation and contribution of IT security professionals.

5.2.4 Maintain vendor neutrality

It is accepted that a each vendor is in the best position to define the knowledge requirements for its own products. For the purpose of broad information security skills accreditation, it was proposed that any certification should be vendor-neutral, although broad platform-specific (ie. Windows, Unix/Linux) knowledge would remain important and relevant.

Workshop participants agreed that the solution should not focus on specific vendor products and solutions but should maintain an awareness of the importance of vendor engagement.

5.2.5 Achieve industry acceptance

Regardless of the chosen way forward, industry acceptance would be essential, both by providers and consumers/employers of information security professional services.

Workshop participants agreed that industry must be willing to own and sponsor any agreed new approach in order to maintain relevance and reputation in the market.

5.2.6 Maintain international relevance

Any scheme proposed would need to be internationally recognised, portable, and relevant.

Workshop participants agreed that the solution should not restrict Australian information security professionals from practising on a global scale, nor should it limit the ability of international professionals to practise in Australia.

5.2.7 Continued requirement for due diligence

Certifications do not relieve an employer of their requirement for due diligence in assessing the suitability of a professional for a particular role.

Workshop participants agreed that the solution must not be seen as a replacement for organisational due diligence when selecting a suitable candidate for an information security role.

5.3 CONTENT

One of the items generating the greatest discussion with stakeholders and industry participants was the selection of the body of knowledge to be used for either an Australian scheme, or for a gap analysis of existing schemes. The fundamental question was what the required knowledge base was for an information security professional operating in Australia, and on this point there is considerable divergence of opinion.

5.3.1 Basis

During the initial interview phase of this project some participants suggested that ISO/IEC 17799, and AS/NZS 7799.2 could provide an appropriate body of knowledge on which a body of knowledge could be standardised, particularly as these standards were recognised by Government. However, it was noted that existing bodies of knowledge in certifications such as the CISSP in no way stated requirements contrary to the application of the Australian standards.

Another alternative suggested was the body of knowledge created by the National Security Telecommunications and Information Systems Security Committee of the US National Security Agency, as the curriculum established by this group has been used in the establishment of a number of other bodies of knowledge.

At the workshop, SIFT presented the option of basing the content of the solution on one of the following: ISO 17799, AS/NZS 7799.2, CISSP CBK or NSTISSC 4011. Discussion led to an understanding that there could be no agreement on a 'body of knowledge until job skills within information security had been identified.

5.3.2 Developing Regional Knowledge

In the initial interview phase, certification bodies were asked if there was any intention of 'regionalising' current certifications available to Australia.

$(ISC)^2$ was uncertain whether a regionalisation of the CISSP program would be financially viable in Australia but said it would be both more effective and economic to use existing internationally accredited certification schemes than to develop a new scheme from the ground up.

A director of SANS and GIAC, noted they would be happy to work with the industry to regionalise existing certifications if there was a committed level of training/certification seats per year.

Industry groups and representatives were asked what the ideal method of integrating regional knowledge was for information security professionals. Both small business representatives and larger companies agreed that extending international accreditation schemes to incorporate required Australian components was preferable to developing a new Australian scheme from the ground up.

5.3.3 Stratification of Certifications

Due to the breadth of the information and IT security industries, broad certifications are now moving to specialisations and other mechanisms to 'stratify' the membership. Various levels have been proposed for such stratification, including:

- Industry (eg, banking & finance, telecommunications, government)
- Management/technical focus
- Job role (eg, architect)
- Required skill set (eg, investigations).

In addition to this, it was suggested that certification and professional association membership should occur at the broad ICT industry level rather than for specialisations such as security.

The approach to having ICT industry level professionalism and certifications (as opposed to moving directly to a security specialisation) was proposed by some participants on the basis that resolving the broader professionalism question before moving to specialist areas could improve the end result.

It was noted that any Australian certification or accreditation scheme would require contextualisation based on the industry to which it related. For example, critical infrastructure organisations were more likely to require an additional degree of knowledge or background checks.

(ISC)^2 indicated that additional competencies that may require certification include forensics, critical infrastructure protection, privacy, governance, risk management and compliance. SANS and GIAC similarly indicated that current programs were "only scratching the surface" of available competency areas. Such comments suggest that over time there will be an increase in the number of certifications available and the scope of roles covered by such certifications.

Workshop participants observed that a clearer understanding was needed within the market of the available roles in information and IT security, and the necessary skills that match each role. Certification was seen to fit in through providing an assurance of a baseline level of knowledge for specific skills that would match identified specific roles.

5.3.4 Re-certification and continuing professional education (CPE)

During the initial interview phase, participants were asked for their views on the need to incorporate re-certification and continuing professional education as part of the solution.

Participants noted that while the continuing professional education of personnel in appropriate legal and regulatory issues may be a requirement, they differed in their views of whether CPE should be a requirement of ongoing certification.

(ISC)^2 suggested that such mandated CPE credits would be appropriate where a certification program was developed with localisation in mind but would be inappropriate for the international programs. Others noted that given the immaturity of the field, mandating certain areas of CPE study (eg, legal and regulatory) would not be recommended.

Workshop participants were neutral with regards to the issue of re-certification and offered no additional comments.

5.3.5 Trustworthiness and clearances

Many organisations identified the issue of trustworthiness as one of the key challenges in the information security marketplace, but an equal number indicated that this is not the responsibility of a certification program.

It was suggested that due to the small size of the information security industry in Australia, it could be feasible to establish a "web of trust" where a series of referrals could provide a suitable approach to trustworthiness. Such an approach could utilise a board panel of review, and supervisor's reports for completed projects. It is acknowledged, however, that such an approach would have considerable confidentiality implications and administrative overheads.

It was noted as the information security profession in Australia was small and, particularly for senior roles, the network of professionals is very good, allowing for a suitable degree of competence and trustworthiness assessment based on trusted referees was a feasible concept.

It was proposed that the development of a 'personnel security' standard could ease the difficulty many organisations face in determining what checks can and should be conducted. Standards Australia confirmed that it was considering the issue of background checks but did not have definitive view at this stage.

A certification for trustworthiness could be considered, similar to models in the US where individuals can submit themselves to an independent board for vetting.

Through further discussion it was determined that the issue of 'standardised' clearances related to support for organisations in undertaking due diligence on personnel for key roles.

5.4 PROPOSED APPROACHES

5.4.1. Degree of Support

Workshop participants were presented with the following diagram of the possible approaches and the respective levels of support across the industry.

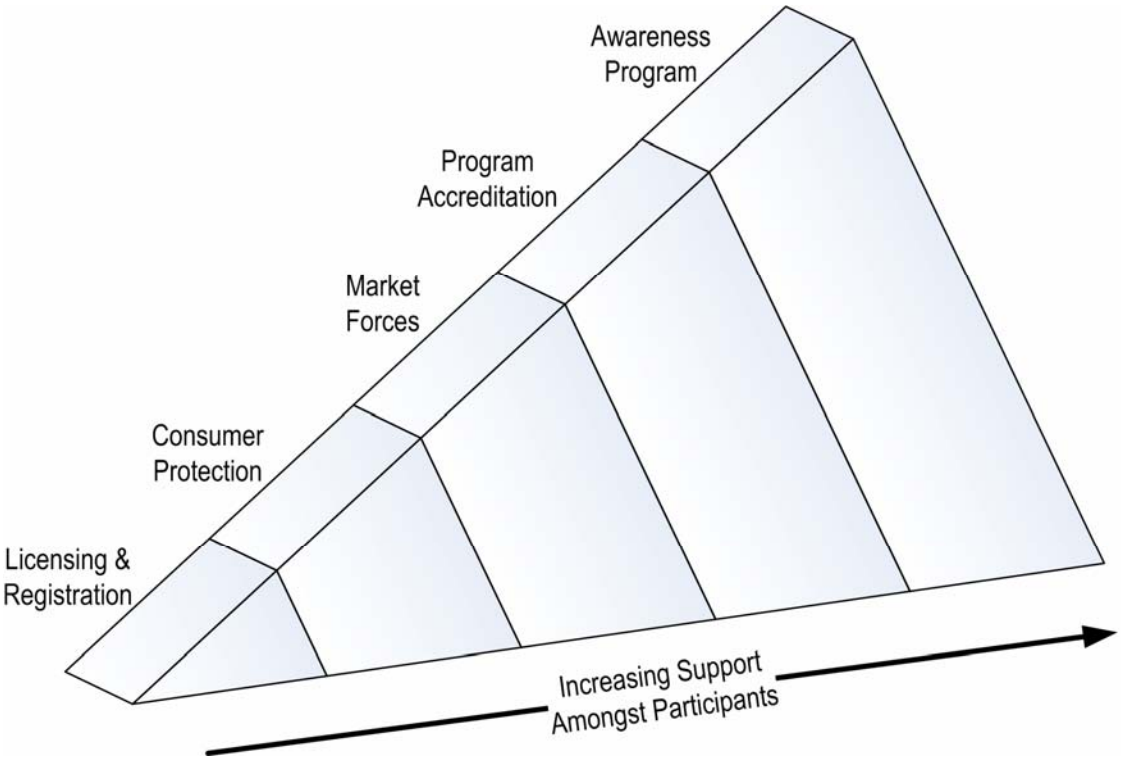


Figure 2: Proposed approaches and levels of industry support

Participants indicated a strong belief that one of the primary issues in the market was a lack of understanding of the relevance of the existing certification programs to different industries, job roles and technical and business environments. As a result, there was considerable support within Government, professional bodies and large and small private sector organisations for an awareness program to provide clarity for consumers/employers/end-users.

Based on the interviews conducted and the workshop discussion there is very little support within industry, either from the information security professional service providers, or from the end-users of such services for a mandatory licensing or registration scheme of any kind.

Some participants had the view that given the immaturity of the information security skills market certification is best left to market forces at this stag.

Other participants suggested a 'program accreditation' structure to provide for the maintenance of consistent standards between competing certification schemes. Such a program accreditation, also described by some as a 'meta-certification', itself has many variables in its implementation, such as the need for a governing body (and if required, the

identity of such a body), and any additional requirements placed on top of the need to simply obtain an accredited certification. Such requirements were generally suggested to include elements of regionalisation, optional specialisation and detailed ongoing industry involvement and continuing education requirements.

The final broad category of suggested governance structures was for the use of existing, or refined, consumer protection mechanisms to improve the quality and consistency of services in the area of information security.

There was consensus among workshop participants that the relative acceptance levels of the five approaches were indicated correctly, with the awareness program deemed as most appropriate to requirements. Participants at the workshop also agreed that an Australian information security skills accreditation scheme was not an acceptable solution for the needs of industry and the marketplace.

5.4.2. Licensing and Registration

It was suggested that a licensing and/or registration program should be put in place for information security professionals, particularly those working with safety critical systems.

However, the vast majority of organisations interviewed during the project were strongly opposed to any attempt to mandate a specific scheme or to create any form of prescriptive regulation in the information or information security skills markets.

As participants clearly indicated that such a scheme would not receive market support either from suppliers or consumers of information security professional services, it was recommended that this not be further considered.

Workshop participants were not supportive of the licensing and registration model for a solution.

5.4.3. Consumer Protection

As one of the drivers identified for the information security skills accreditation program was the need to ensure small to medium enterprises were receiving quality services, it was proposed that standard employment contracts could be used to provide some consistency.

It was suggested that some participants that consumer law could afford some level of protection for SMEs acquiring information security services. There was however agreement that standard employment contracts alone could not ensure that professionals were able to meet individual organisation's requirements.

It was similarly noted that the utility of consumer protection mechanisms such as standard form contracts was minimal as the large consumers/employers of information security professional services will generally use internal legal and compliance personnel and associated contracts.

5.4.4. Market Forces

A number of interview participants made the point that allowing market forces to dictate the direction of accreditation and certification is an important alternative to consider.

A number of organisations suggested that many of the issues being discussed were 'growing pains' as the information security field matured. As standard practices and procedures were put in place, and as a better understanding of professionalism in this context was developed, the accreditation/certification issues would be resolved.

Many users of information security professional services indicated that they do not enforce a requirement for qualifications in the field, as unqualified practitioners have often proved to be exceptional information security professionals. It is expected that irrespective of the establishment of a new certification/accreditation scheme, companies would continue to recruit personnel outside of this scheme where they were considered to be the best candidate.

Organisations have identified that university graduates with certifications often lack practical and operational experience. However, it was felt that this analysis of practical and operational experience would be handled through existing recruitment and interview processes, rather than attempting to use a certification program for this purpose.

$(ISC)^2$ noted that current market needs have generated several internationally recognised information security personnel certifications and future needs were currently generating the development of others. TAFE NSW similarly indicated that it was often better to maintain an 'open' approach to standards and to allow the market to fill the need.

AITSF said that from an information security industry perspective, its preferred option would be to let the market decide, and that most organisations were happy with the international certifications available.

The reaction from the workshop towards market forces driving the solution was very positive. It was noted by participants that a demonstrated amount of information and effort has been contributed to current information security skills accreditation by market forces. The identified opportunity would be to supplement market forces to achieve a degree of consistency and maturity in the information security marketplace sooner than would otherwise be achieved.

5.4.5. Program Accreditation

During the interview phase of the project, there was considerable discussion around the relative benefits of certifying individuals, or accrediting certification providers. It was believed that that quality could be assured through a board or council providing accreditation of the program itself.

It was proposed that an accreditation (umbrella) organisation could be established utilising a JAS-ANZ-type accreditation process, with the certification bodies underneath, thus providing assurance of the certification process. Since accrediting certification bodies would be likely to be process-intensive, it would be necessary to demonstrate significant value for the certifying organisations to get them on board. However, not all participants agreed with this proposal. Participants questioned the benefits of having an additional level of bureaucracy.

It was agreed that 'unification' of existing certifications into a single Australian scheme is unlikely, both due to the commercial drivers of the certification bodies and the needs of specific areas of the industry. For example, it is expected that DSD will continue to operate the I-RAP program regardless of other programs put in place, due to the nature of the work and Government control of the relevant standards (ACSI 33 and the Protective Security Manual).

As the "program accreditation" approach has the potential to introduce significant complexity, the following sections examine the key issues in more detail, specifically with respect to the ISO 17024 standard which was raised as a possible standard for the program accreditation approach.

5.4.5.1. Mutual recognition requirements

One suggestion was that the US Free Trade Agreement (FTA) should be considered for its impact on any Australian scheme. Standards Australia similarly noted the importance of ensuring that any Australian scheme does not introduce any restraints to trade.

The Department of Education, Science & Training (DEST) advised that there is a key principle of mutual recognition embedded in the US FTA and other World Trade Organisation (WTO) relationships. DEST suggested close analysis of any requirement that would make it harder for overseas professionals to practise in Australia. Any such requirement would need to be clearly justified on the basis of safety, quality or efficacy.

The use of international standards such as ISO/IEC 17024 is seen as a useful mechanism for ensuring this international consistency and providing both for Australian professionals to work internationally and for overseas professionals to support Australia's information security needs.

5.4.5.2. Ensuring certification quality

During the initial interview phase, the importance of ensuring the experience and relevance of teachers in this field was raised as well as the qualifications, knowledge and experience of teachers and trainers in the information security field.

There were differing views on whether industry or academia made for better teachers. One view was that as most tertiary education departments require a doctorate in a relevant discipline before being allowed to teach, educational qualification requirements in academia are therefore higher than in industry.

There is a belief that current certifications have too much reliance on questions and answers, and there would be benefits in additional face-to-face assessments by a panel for industry certifications. This would assess the ability for individuals to think on their feet and ability to communicate.

ACS, $(ISC)^2$, ISACA and ISSPCS all acknowledge the relevance and requirement of achieving accreditation to ISO/IEC 17024-2004: *Conformity assessment – General requirements for bodies operating certification of persons*.

ISACA noted that any program accreditation scheme needed a mechanism for recourse, a transparent assessment process and consistently high standards. It was acknowledged by all participants that the international standard and relevance of any program put in place would be paramount.

AITSF noted that while ISO/IEC 17024 would provide a genuine measure of the integrity of the certification process, it was important to consider other implications:

- Achieving compliance to the standard, and being accredited against it, can introduce significant cost that is then passed on the consumer/employer; and

- Accreditation verifies the integrity/suitability of the certification process, not the content.

At the workshop the point was raised that the point that Australia has two organisations already accredited to ISO/IEC 17024, in fields unrelated to information security and the mechanisms for developing such a scheme for information security are already in place should industry wish to formalise such a scheme at a point in the future.

5.4.5.3. Recognition of prior learning (RPL) and prior experience (RPE)

Organisations differed in their views on the value and importance of including experience as a requirement of a certification program. This topic was not discussed at the workshop due to time constraints and as it was not raised as a key issue.

It was proposed that any new Australian certification or accreditation program would require a 'grandfathering' scheme and an acceptance of recognition of prior learning and recognition of prior experience processes. Such a requirement would introduce the need for a governing board or panel which would be responsible for conducting assessments. Peer verification of experience was noted as being important.

Significant pitfalls to be avoided included the tendency to 'grandfather' applicants who had not proven their skills and too much weight being given to experiences that did not validate the individual's capability to complete a given job.

(ISC)^2 and ISACA also noted that in determining competence, experience was required beyond security skills, including general management, budgeting, people skills, presentation skills, and other areas. These areas were best validated through existing human resources and recruitment processes.

It was suggested that an equivalence process of current international certifications should be made available to Australian citizens, certifying an Australian knowledge base. Migrant professionals should go through a skilled process to attain this Australian-specific knowledge. As the focus of discussions for this project was on information security skills certification programs available in Australia, and this issue was not raised by any other project participants, the issue of recognising national programs originating outside Australia was not examined further.

At this stage, industry is supportive of the use of the ISO/IEC 17024 standard to provide for a consistent level of process maturity and integrity in the information security skills accreditation field. However, participants did not see a need for there to be a requirement for a formalised "scheme", nor for the use of a governing body to oversee such a process. Discussion around the need for a governing body is dealt with in more detail in section 5.4.7.

5.4.6. Awareness Program

Following the workshop meetings further discussions were held with stakeholders on the broad issue of raising market awareness of information security skills accreditation. Three key areas or elements of an awareness program to support both small and large enterprises were identified:

- Awareness of the qualifications available and their relevance/content;

- Support in defining the requirements for an information security role or project; and
- Support in determining the appropriate checks to be conducted in performing due diligence on a potential employee or contractor/consultant.

All certification bodies and professional associations agreed that there is a need for better awareness in the market of the meaning of the currently available certification programs. The need for more advertising, awareness and developing brand awareness of information security professional qualifications was highlighted

A number of organisations including ISIG and (ISC)^2 noted a requirement for information security roles to be better defined to allow for more accurately assessing a candidate's fit to the position. However, it was noted that while there may be poor definition of such roles, this was no different to many other professional services fields, such as management consulting.

It was suggested that a simple mapping between vendor certifications and related product and product areas would be of value to the market. This could be extended to be a 'ready reckoner' to identify job functions by certification to help owners and operators of critical infrastructure identify the right professionals easily and quickly in order to protect their systems.

In addition, a 'Buyer's Guide' to IT security professional services would provide a matrix of disciplines to certification/knowledge areas.

There was also general consensus that employers should understand their own requirements to conduct due diligence on any proposed employee, regardless of their certification and experience. It was suggested that a statement/recommendation should be issued to critical infrastructure owners and operators on how to select people in this field. Support to be provided to employers in this area could include providing guidance on the range of background checking mechanisms available, how these are used, and the degree of assurance provided by each.

Workshop participants emphasised the need to lift the level of awareness so consumer/employers and professionals both have a better understanding of the complexity of certification and recruitment within the information security industry. There was also a requirement for professional organisations to leverage the power of any awareness program and distribute the knowledge to the consumers/employers of information security services.

5.4.6 Governing Body

During the initial interview phase, participants were asked how an information security skills accreditation scheme for Australia should be structured. Participants had varying views and different types of governance were proposed by participants

At the workshop however, participants reached a consensus that an information security skills accreditation scheme was not deemed as an appropriate solution to the issues raised. Therefore the topic of a governing body was only briefly touched on, and participants indicated a reluctance to support it.

5.5 DEMAND AND SUPPLY DRIVERS

5.5.1 Driving Acceptance

It was important to ensure current industry practitioners, both with and without certifications, were in a position to work with any scheme developed. It was clearly indicated by representatives of information security practitioners that personnel with current international certifications are unlikely to pursue an additional certification.

It was noted that Australia needs to attract overseas talent and forcing them to locally certify in addition to international certifications may prove to be a deterrent. A similar challenge is that of gaining critical mass for an Australian certification when competing against international certifications with a significant head-start.

5.5.2 Cost

Participants indicated that the cost of any new accreditation process needed to be at a level that would not increase the cost of information security professional services across the market.

Specific cost issues were not investigated but it was noted that ensuring no undue financial burden was placed on information security professionals, or the organisations using their services, was one of the generally accepted principles.

5.5.3 Structural change

It was frequently noted that the information security professional services market in Australia is fragmented and as such contains many individuals operating as either sole traders or in loose affiliations with others. It was suggested by some interviewees that this structural component of the industry could either be intentionally modified to provide greater control or could unintentionally be modified through the implementation of an accreditation scheme.

While this is not currently proposed as a specific option, it is however included for completeness and to remain cognisant of potential flow-on effects.

6 CONSENSUS

Following from the workshop, further consultations with key industry groups and certification bodies were held to provide greater clarity around the specific 'solutions' being put forward. Two specific items receiving the greatest support were:

- An Awareness Program on existing certifications
- An Australian Training Component for existing certifications

These two items are discussed in greater detail in the following sections.

6.1 CONSENSUS TOWARD AN INDUSTRY AWARENESS PROGRAM

Discussions following from the workshop took place to construct an overview of what an Awareness Program should encompass, in order to determine how organisations, professionals and consumer/employers could gain the greatest benefit from its development.

6.1.1 Objectives of an Industry Awareness Program

Participants were asked to highlight objectives an Awareness Program should seek to achieve in order for it to be relevant to the information security industry as a whole.

1. The Awareness Program should provide a validation of certification quality along with detail on certification content in order to assist information security professionals in selecting the appropriate certification for their job role and career.
2. The Awareness Program should provide an accepted point of reference with which to compare and contrast certification schemes currently available.
3. The Awareness Program should increase the confidence level of consumer/employers in knowing when help is required for information security, and where to find the right professionals to do the job. Subsequently, the Awareness Program should help organisations to realise that security is an on-going process which involves selecting the right professionals from the start.
4. In order to maintain vendor neutrality, the Awareness Program should not promote specific certification schemes. The Awareness Program should serve the role of informing consumer/employers and professionals to allow them to decide on the most appropriate program for their needs.
5. The Awareness Program should include sources of knowledge which may not be referenced by current certifications, such as new and accepted references to best practice.

6.1.2 Delivery Medium

A number of organisations in the initial interview phase proposed the concept of a Buyer's Guide as the medium for disseminating the required information to professionals and

consumer/employers. Participants agreed that the Buyer's Guide should contain information covering the following:

6.1.2.1 IT Security vs. Information Security

The Buyer's Guide must differentiate and explain the differences between IT security and information security to consumer/employers and professionals, to support the correct definition of the required skill set for a given role.

6.1.2.2 Roles and Responsibilities

The Buyer's Guide must clearly define job roles and responsibilities within the information security industry to provide a common guideline for information security professionals practising in Australia. A framework of generally accepted knowledge and skills for specific information security roles, particularly information security managers, should be included in the Buyer's Guide.

ISSA is currently undertaking an identification mapping process for roles and responsibilities within the information security industry and is willing to contribute its knowledge in the area to this effort. ISACA and $(ISC)^2$ have both independently been involved in developing a career road map for information security professionals. $(ISC)^2$ is still involved in similar efforts around the world and is willing to share lessons learnt from the exercise. ISACA, however, has stated that their initiative in the past has had limited success due to the issue of identification and 'naming' of roles within the information security industry globally. ISACA are currently developing a functional job specification for "Information Security Manager". Comments made in regard to positional titles are related not to tasks performed, but labels that are given to those that undertake the tasks in different global locations. As job titles are generally company specific, $(ISC)^2$ has recommended that the exercise include a task set for each job role to avoid any confusion or misrepresentation.

6.1.2.3 Qualifications Guideline

The Buyer's Guide should outline the current qualifications available to information security professionals and identify areas of similarity and difference between them. The list of qualifications should include information security programs offered by certification bodies, various educational institutions and universities. Content should be easily comprehensible and should summarise the skills and knowledge examined as well as the requirement for continuing professional education by each qualification to provide a guideline for consumer/employers and professionals.

6.1.2.4 ISO/IEC 17024 Accredited Certificates

The Buyer's Guide should inform consumer/employers and professionals on ISO/IEC 17024 and its role in providing a quality assurance benchmark for certification bodies. The Buyer's Guide should outline the scope of ISO/IEC 17024 and provide information on the criteria for certification bodies in the development and maintenance of certification schemes. The Buyer's Guide should include a list of ISO/IEC 17024 accredited certification schemes.

6.1.2.5 Qualifications Mapping

Qualifications mapping was the most requested component by industry professionals and consumer/employers of a proposed Buyer's Guide. The qualifications mapping should indicate

the technical abilities and management skills covered by qualifications. It should also match certifications to specific job roles.

The purpose of the qualifications mapping would be two-fold. Firstly, consumer/employers will be better informed on skills and qualification requirements when recruiting for an IT security role. Secondly, information security professionals will have a relevant reference for choosing and comparing qualifications for their own professional education and development. The qualifications mapping would be a critical component of the Buyer's Guide as it would demonstrate that various certifications address different skill and role requirements. In order to maintain vendor neutrality, it was agreed by industry groups that the qualification mapping of available certifications against recognised information security skills should be completed by external parties as opposed to certification bodies.

6.1.2.6 Directory of Contacts

The Buyer's Guide should include a directory listing of contacts for the certification schemes currently available. The directory should maintain the latest information available for the definitive contacts of certification bodies and include details such as head office location, website address, phone and fax numbers.

6.1.2.7 Due Diligence

The degree to which guidance on due diligence should be included in the Buyer's Guide was not agreed across all participants.

While educating the market on available services and approaches for conducting due diligence was considered a worthwhile endeavour, it was felt that this should not be a core component of the information security skills accreditation awareness program.

6.1.2.8 Suggested Content

While the majority of content areas were agreed at a high level, such as details on the available certifications, the inclusion of information on ISO 17024, and the appropriateness of each certification for given job roles and careers, other areas of content was suggested as adding value to the guide.

It was suggested that the Awareness Program include

- an explanation on Control Objectives for Information and Related Technology (COBIT),
- the Information Technology Infrastructure Library (ITIL) in relation to certifications,
- basic information on issues such as privacy,
- the Sarbanes-Oxley Act and its impact on Australia, and
- other governance and compliance drivers,
- the relevance of certifications being governed by a Code of Ethics and standards.

It is agreed that all the above items would provide valuable information to both consumer/employers of information security services and information security professionals themselves. However, it was also acknowledged that it is important to ensure the Buyer's Guide does not attempt to solve all information issues in the industry at once. Inclusion of

information outside of the core functions of the Buyer's Guide should be discussed by the participants and topics included sparingly.

6.1.3 Participation

For this phase of the project, the following organisations were selected for further consultations:

- AITSF
- AusCERT/ISSPCS
- (ISC)^2
- ISACA
- ISIG
- ISSA
- QUT
- SANS.

Resources and other competing priorities permitting, all of the participants interviewed were keen to contribute industry experience and knowledge towards developing and administrating the Awareness Program. However, participants also identified the need to negotiate the level of involvement expected from each stakeholder in the Awareness Program. Details such as funding, resourcing and timeframes would need to be considered between all organisations involved in the Awareness Program. Organisations were also willing to promote the Awareness Program provided the content was appropriate.

6.2 CONSENSUS TOWARDS A TRAINING COMPONENT

In conjunction with the Awareness Program, an Australian training component was proposed as a solution to address the lack of regional knowledge faced by professionals who practise in the Australian information security environment. After the workshop, key industry group members and certification body representatives were consulted to construct an overview of what the Australian training component should encompass in order to meet the needs of industry.

6.2.1 Objectives

Participants were asked to identify objectives the Australian training component should seek to achieve in order for it to be valuable and useful to information security professionals.

1. The Australian training component should address the lack of knowledge in the area of legal and regulatory matters in the Australian work environment. However, it was observed by all participants that the Australian training component should be developed with the understanding that information security professionals should not be experts on legal and regulatory matters.
2. The Australian training component should validate that the legal information and advice provided to information security professionals by lawyers is appropriate.

3. The Australian training component should be an optional choice for information security professionals in Australia and it should be economically priced.

6.2.2 Content

Participants were asked to identify topics which are specific to Australia and require better coverage in order for information security professionals to have a better understanding of the domestic information security environment.

6.2.2.1 Legal and Regulatory

The Australian training component should cover the essential knowledge of practising information security within the context of Australian regulations and legislation such as the *Privacy Act 1988*. Professionals undergoing the Australian training component should gain an understanding of the requirements of local legislation and regulation. It was that while information security professionals would then be familiar with the Australian legal and regulatory framework they would remain unable to offer professional legal advice in this field.

Industry groups have suggested that the Australian training component should also outline the relevance of international legislation, such as the Sarbanes-Oxley Act 2002, in the Australian information security environment.

6.2.2.2 Code of Ethics

As part of the Australian training component, SANS has recommended Australia set a precedent by presenting a standard Code of Ethics for information security professionals which can be practised globally. However, it has been observed by ISACA that most certification bodies already have their own Code of Ethics by which certified professionals are obliged to abide. $(ISC)^2$ observed that the ethics requirements are unlikely to vary from country to country and ethical practices in Australia would not be different from internationally accepted practices.

6.2.2.3 Social and Cultural

Participants were asked if topics like Australian social and cultural issues should be addressed by the Australian training component. Participants from industry groups decided against including social and cultural issues, and certification bodies offered support only if the inclusion of social and cultural issues were deemed necessary by industry.

6.2.2.4 Australian Standards and Guidelines

SANS has suggested that it would be appropriate for the Australian training component to explain the relevance of Australian security guidelines such as the Australian Government Information and Communications Technology Security Manual (ACSI 33). Another standard put forward for inclusion in the Australian training component is the Australian Government's Protective Security Manual (PSM) however it is noted that this standard is not publicly available.

6.2.2 Participation

For this phase of the project, the following organisations were selected for further consultations:

- AITSF
- AusCERT/ISSPCS
- (ISC)^2
- ISACA
- ISIG
- ISSA
- QUT
- SANS.

However, not all organisations agreed to be involved with the development and administration of the Australian training component.

AITSF has declined to be involved as a major stakeholder in the Australian training component initiative as it believes that an international perspective is more crucial to an effective program than is an Australian training component.

Organisations which did agree to be involved with the Australian training program again asserted the need to negotiate the level of involvement for each stakeholder. For the certification bodies, it was important to distinguish ownership of material contributed to the Australian training component and ensure accuracy of the localised content.

6.2.3 Competition

A potential model discussed for the Australian training component was for the component to be collaboratively developed by interested stakeholders, and to be incorporated – formally or informally – into existing certification and qualification schemes. The inclusion of the Australian component in the examination/certification stage was not assumed, however through the inclusion of this material in the supporting training programs, an opportunity will exist for Australian information security professionals to be exposed to this information.

It is not proposed that the Australian training component would compete with existing certifications rather it would be an additional body of knowledge offered by existing certification providers. Certification bodies were asked at interview if they would be willing to support such a component.

SANS has agreed in principle not to compete with the Australian training component and will promote such a program to information security professionals on the condition that the material presented in the program is of high quality.

Although ISACA does not view competition as an issue, it has reserved final judgment until the content and context of the Australian training component are known. ISACA has requested clarity and definition on the purpose and intention of the Australian training component as well as areas of the material that may be covered by existing programs.

It was observed that ensuring the content taught in the Australian training component does not conflict with current certification material will be difficult to achieve if a consensus is not

reached by industry and certification organisations. While consensus is not impossible to achieve, it may become a barrier to the progress of the Australian training component. Furthermore, as certification schemes evolve and improve, there could be overlap between topics covered by the Australian training component and certification schemes.

(ISC)^2 believes it is not in the interests of the information security community to have duplication of effort and says the Australian training component should not compete with existing training, education and certification products. (ISC)^2 observed that it would be difficult to exclude itself from providing educational products that could help in the development of its Australian constituents. The exact nature of the Australian training program and how it fits with the (ISC)^2 charter will dictate the level of (ISC)^2 participation.

7 APPENDIX A: PARTICIPANTS

The following is a list of organisations approached to partake in this project. Organisations shaded declined to be involved in this project.

ORGANISATION	REPRESENTATIVES	SECTOR
ACIF – Australian Communications Industry Forum		Industry organisation for facilitating communications self-regulation
AGIMO – Australian Government Information Management Office	s47F	Federal Government
AGL – Australian Gas Light Company		Critical Infrastructure
AHTCC – Australian High Tech Crime Centre		Law Enforcement
ANZ Bank		Banking and Finance
AIIA – Australian Information Industry Association	s47F	Industry organisation for Information and Communications Technology
AOEMA – Asia Oceanic Electronic Marketplace Association		Industry and consumer organisation for the development and use of secure global e-commerce
AGD CIP – Attorney General's Department Critical Infrastructure Protection Branch		Federal Government

ORGANISATION	REPRESENTATIVES	SECTOR
AusCERT & ISSPCS – Australian Computer Emergency Response Team	s47F	Certification bodies
ABA – Australian Bankers' Association		Industry organisation for the development of public policy on banking and other financial services
Australia Post		Critical Infrastructure
ACCI – Australian Chamber of Commerce and Industry		Council of Australian business associations
ACS – Australian Computer Society	s47F	Association for Information and Communications Technology professionals
AITSF – Australian IT Security Forum		Forum for promoting information security within the Australian information economy
Bridge Point Communications		Provider of Information Security Consulting, Training and Network Integration services

ORGANISATION	REPRESENTATIVES	SECTOR
Centrelink	▪ s47F	Critical Infrastructure
CISCO		Product vendor
CBA – Commonwealth Bank of Australia	▪	Banking and Finance
DSD – Defence Signals Directorate		Federal Government
EA – Energy Australia		Critical Infrastructure
eSecurity Australia	▪ s47F	Industry organisation for e-security in Brisbane
Hutchison Telecommunications	▪ ▪	Telecommunications
IIA – Internet Industry Association	▪	Industry organisation for providing policy input to government
ING Australia	▪	Banking and Finance

ORGANISATION	REPRESENTATIVES	SECTOR
ISACA (Sydney Chapter) – Information Systems Audit and Control Association	s47F	Certification body
(ISC)² Asia-Pacific – International Information Systems Security Certification Consortium		Certification body
ISIG – Information Security Interest Group		Industry organisation for promoting awareness and understanding of information security issues
ISSA – Information Systems Security Association		Industry organisation for promoting information security best practices

ORGANISATION	REPRESENTATIVES	SECTOR
JAS-ANZ – Joint Accreditation System of Australia & New Zealand	s47F	Joint accreditation body for Australia and New Zealand
Macquarie University		Education
Microsoft		Product Vendor
NAB – National Australia Bank		Banking and Finance
PSC – Professional Standards Council		State Government
QUT – Queensland University of Technology		Education
RMIT University – Royal Melbourne Institute of Technology		Education
SAI Global		Provider of business publishing, training and assurance services
SANS Institute		Certification body
SETEL – Small Enterprise Telecommunications Centre Ltd		Consumer organisation for the advancement of telecommunications and e-commerce of Australian small business

ORGANISATION	REPRESENTATIVES	SECTOR
SingTel Optus	s47F	Telecommunications
Small Business Coalition		Industry association for interest in small business issues
St George Bank		Banking and Finance
Standards Australia	s47F	National standards body
Sydney Water		Critical Infrastructure
TAFE NSW	s47F	Education
Telstra		Telecommunications
Vodafone		Telecommunications
Westpac Bank		Banking and Finance

8 APPENDIX B - SUMMARY OF PARTICIPATING ORGANISATIONS

The following diagram illustrates the spectrum of industries and industry sectors involved in this project.

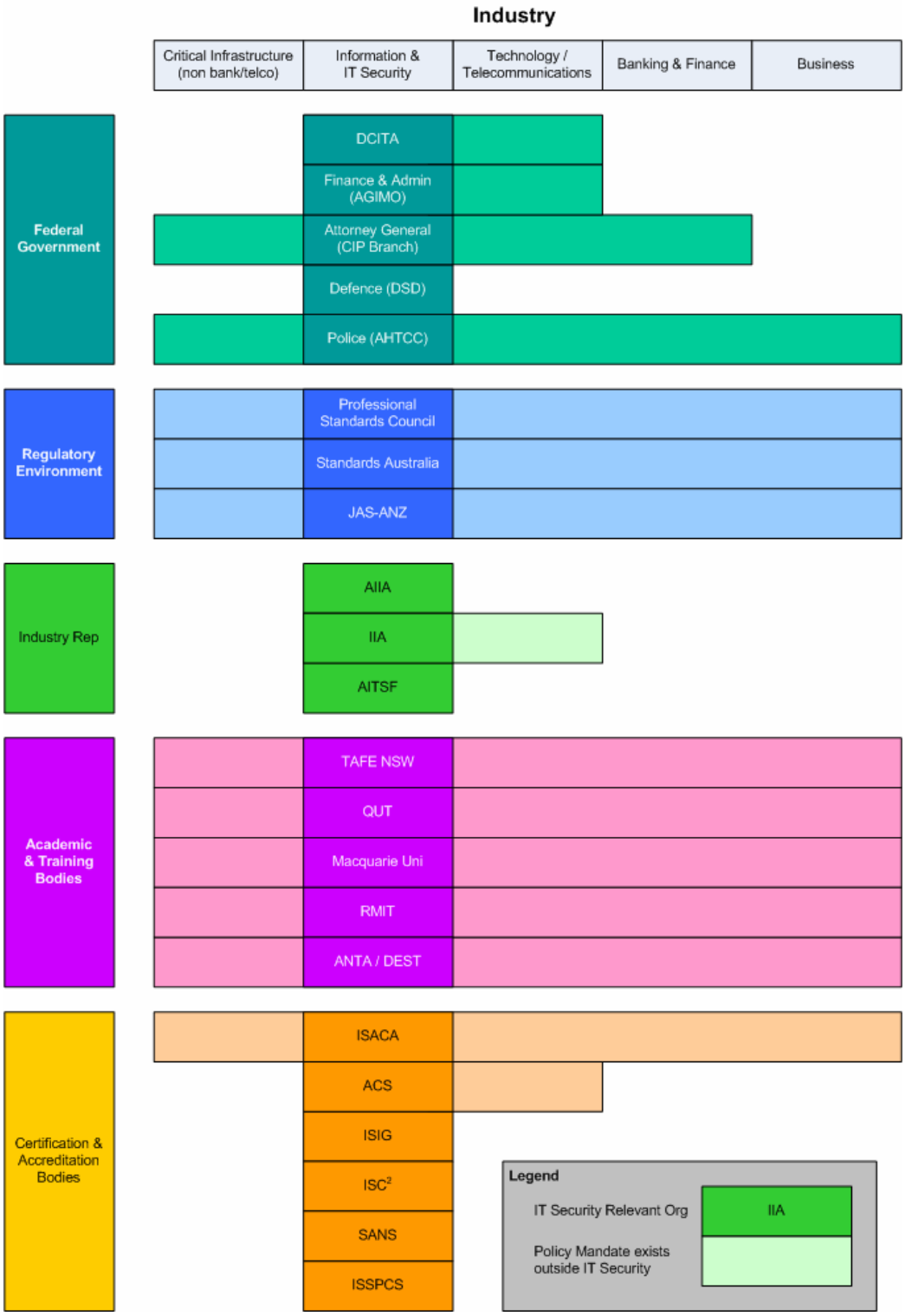


Figure 3: Spectrum of industries and sector areas

AGIMO – Australian Government Information Management Office

The Australian Government Information Management Office (AGIMO), Department of Finance and Administration is working towards making Australia a leader in the productive application of information and communications technologies to government administration, information and services. AGIMO provides strategic advice, activities and representation relating to the application of ICT to government administration, information and services.

URL: http://www.agimo.gov.au/about

AGL – Australian Gas Light Company

AGL has been a major participant in the Australian energy industry since 1837. Today AGL is a major retailer of gas and electricity to about three million customers. AGL also has an extensive portfolio of wholly and partly-owned investments in energy infrastructure, infrastructure management and other energy companies.

URL: http://www.agl.com.au/AGLNew/default.htm

AHTCC – Australian High Tech Crime Centre

The Australian High Tech Crime Centre's (AHTCC) purpose is to enforce Australian law in combating serious crime involving complex technology. AHTCC is hosted by the Australian Federal Police (AFP) in Canberra and includes representation from all Australian State and Territory police forces, both in its staff and Board of Management.

The role of the AHTCC is to:

- Provide a national coordinated approach to combating serious, complex and multi-jurisdictional high tech crimes, especially those beyond the capability of single jurisdictions;
- Assist in improving the capacity of all jurisdictions to deal with high tech crime; and
- Support efforts to protect the National Information Infrastructure.

URL: http://www.ahtcc.gov.au/

AIIA – Australian Information Industry Association

AIIA is a representative body in Australia for the Information and Communications Technology (ICT) industry. AIIA works across many areas to assist the ICT industry to meet its business objectives in corporate and government markets.

URL: http://www.aiia.com.au/i-cms.isp

AOEMA – Asia Oceanic Electronic Marketplace Association

The Asia Oceanic Electronic Marketplace Association (AOEMA) is a not-for-profit organisation which develops the use of secure global electronic commerce. AOEMA has been working with

the APEC Telecommunications and Information Working Group since its inception and provides services to assist small and micro enterprises in all countries in the region.

URL: http://www.aoema.org

AGD CIP – Attorney-General's Department Critical Infrastructure Protection Branch

The Critical Infrastructure Protection Branch of the Attorney-General's Department is responsible for the development and coordination of Australian Government policy and international cooperation relating to critical infrastructure protection, including the National Information Infrastructure (NII). The branch also provides general and legal policy advice and coordination within the department on e-security (including its relationship to high-tech crime), and cyber-terrorism.

URL: http://www.ag.gov.au/agd/WWW/securitylawHome.nsf/Page/Critical_Infrastructure

AusCERT – Australian Computer Emergency Response Team

AusCERT is the national Computer Emergency Response Team for Australia. As a trusted Australian contact within a worldwide network of computer security experts, AusCERT provides computer incident prevention, response and mitigation strategies for members, a national alerting service and an incident reporting scheme.

URL: http://www.auscert.org.au/

ACS – Australian Computer Society

The Australian Computer Society (ACS) is a representative association for Information & Communications Technology (ICT) professionals in Australia. The society has a large and active membership from all levels of the ICT industry. A member of the Australian Council of Professions, the ACS is a public voice of the ICT profession and an advocate of professional ethics and standards in the ICT industry, with a commitment to the wider community to ensure the beneficial use of ICT.

URL: http://acs.org.au/

AITSF- Australian IT Security Forum

The mission of the Australian IT Security Forum is to promote information security within the Australian information economy, through the development of associated technologies, capabilities and services, and to advance the Australian information security industry internationally.

URL: http://www.aitsf.aeema.asn.au/

Bridge Point Communications

Bridge Point is a provider of both Information security consulting, training and network integration services. Since commencing operations in Brisbane, Australia in 2000, Bridge Point has developed a team of experienced consultants and engineers who have successfully completed a wide range of information security and networking projects.

URL: http://www.bridgepoint.com.au

Centrelink

Centrelink is a government agency delivering a range of Commonwealth services to the Australian community. Centrelink's inception was motivated by the amalgamation of community service agencies to provide a central point of contact.

URL: http://www.centrelink.gov.au

CBA – Commonwealth Bank of Australia

The Commonwealth Bank of Australia (CBA) is one of Australia's largest financial institutions with businesses in New Zealand, Asia and the United Kingdom. CBA provides banking and financial services for all Australians.

URL: http://www.commbank.com.au/default.asp

DSD – Defence Signals Directorate

The Defence Signals Directorate's purpose is to support the Australian Government decision-makers and the Australian Defence Force with high-quality foreign signals intelligence products and services. The DSD ensures certainty and effectiveness in Government and Defence policies by providing important information that is not available from open sources to policy departments and assessment agencies. The DSD also provides a range of information security services to the Australian Defence Force and Australian Government agencies to ensure that their electronic information systems are not susceptible to unauthorised access, compromise or disruption.

URL: http://www.dsd.gov.au

eSecurity Australia

eSecurity Australia is an unincorporated cluster of approximately 35 e-security related organisations. The group was formed in early 2001 in Queensland, Australia.

URL: http://www.esecurityaustralia.com/

Hutchison Telecommunications

Hutchison Telecommunications (Australia) Limited is a mobile communications company, offering Australian mobile consumers a choice of services from two distinct global brands, Orange and 3.

URL: http://www.hutchison.com.au

IIA – Internet Industry Association

The Internet Industry Association is Australia's national internet industry organisation. Members include telecommunications carriers, content creators and publishers, web developers, e-commerce traders and solutions providers, hardware vendors, systems integrators, banks, insurance underwriters, technology law firms, ISPs, educational institutions, research analysts, and those providing professional and technical support services.

URL: http://www.iia.net.au

ING Australia

ING is one of Australia's leading fund managers and life insurers with more than $38 billion in assets under management. ING Australia was founded in Sydney in 1878 as Mercantile Mutual. In 1982 it became part of what is now ING Group. ING provides a range of financial products and services through a network of advisers and financial institutions.

URL: http://www.ing.com.au

ISACA – Information Systems Audit and Control Association

With more than 47,000 members in more than 140 countries, the Information Systems Audit and Control Association (ISACA) is a well-recognised IT governance, control, security and assurance organisation. ISACA develops international information systems auditing and control standards and administers the globally respected CISA and CISM certifications.

URL: http://www.isaca.org

(ISC)^2 – International Information Systems Security Certification Consortium

The International Information Systems Security Certification Consortium (ISC)^{22}, is a non-profit organisation. (ISC)^2's main functions are:

- Maintaining the CBK for information security;
- Certifying industry professionals and practitioners under an international standard, Providing education;
- Administering certification examinations; and
- Ensuring the continued competence of credential holders.

URL: https://www.isc2.org

ISIG – Information Security Interest Group

The Information Security Interest Group (ISIG) branches exist in Sydney, Melbourne, Canberra, Brisbane and Adelaide. ISIG currently has more than 200 paid members and more than 500 'friends' on its mailing list. ISIG is an organisation for individuals rather than companies. Membership ranges from company CEOs through to highly skilled technical security specialists.

URL: http://www.isig.org.au

ISSA – Information Systems Security Association

The Information Systems Security Association (ISSA) is a not-for-profit international organisation of information security professionals and practitioners. ISSA provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

URL: http://www.issa.org

ISSPCS Academic Board

ISSPCS Academic Board's purpose is to ensure the ISSPCS certifications stay relevant and focused on current and realistic commercial, governmental and academic interests. The board controls the curricular and assessment aspects of the certification.

URL: http://www.isspcs.org/board/

JAS-ANZ – Joint Accreditation System of Australia & New Zealand

JAS-ANZ is a not-for-profit, self-funding international organisation established under a treaty between the Governments of Australia and New Zealand to act as the joint accreditation body for Australia and New Zealand for certification of management systems, products and personnel.

URL: http://www.jas-anz.com.au/showpage.php

Macquarie University

Macquarie University, situated in Sydney's north-west, has a reputation as an innovator in higher education learning and research. Macquarie has developed and enhanced a high-performance research culture in key areas of environmental science, social sciences, commerce, the humanities (including the Macquarie Dictionary Centre) plus science and technology.

URL: http://www.mq.edu.au/

Microsoft

Microsoft was founded in 1975, with the local Australian operation starting in 1983. An estimated 16 million Australians use Microsoft products from home to the office. Microsoft has a staff of more than 700 people working across Australia, as well as ninemsn, and Microsoft's Home and Entertainment Division.

URL: http://www.microsoft.com/australia

PSC – Professional Standards Council

The Professional Standards Council was established in 1995 under the Professional Standards Act 1994 (NSW) and also later under the Professional Standards Act 1997 (WA). Under the Act, the council's role is to advise, monitor, educate and advocate on issues affecting occupational associations, professionals and consumers in general. PCS's 11 council members come from a variety of professions and disciplines. They are appointed by the Attorney-General.

URL: http://www.agd.nsw.gov.au/psc

QUT – Queensland University of Technology

Queensland University of Technology (QUT) is one of Australia's largest universities, enrolling 40,000 students, 12 per cent from overseas. QUT offers a range of undergraduate degrees, with the flexibility to choose a combination of study areas as well as participate in exchange programs with overseas universities.

URL: http://www.qut.edu.au

RMIT University – Royal Melbourne Institute of Technology

RMIT offers more than 200 TAFE and higher educational programs across a broad range of fields. Traditional strengths such as engineering, business and IT sit beside popular contemporary fields including life sciences, communications and fashion.

URL: http://www.rmit.edu.au

SAI Global

SAI Global Limited is a business publishing, training and assurance organisation with offices in Australia, New Zealand, United States and across Asia. SAI Global delivers an integrated range of standards and business improvement-related products and services ranging from occupational health and safety systems to risk and environmental management training.

URL: http://www.saiglobal.com.au/

SANS Institute

SANS is a provider of information security training and certification around the world. It also develops, maintains, and makes available at no cost, a large collection of research documents about various aspects of information security, and it operates the internet's early warning system -– Internet Storm Center. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs.

URL: http://www.sans.org

SingTel Optus

SingTel Optus provides a broad range of communications services including mobile, national and long-distance services, local telephony, international telephony, business network services, internet and satellite services and subscription television.

URL: http://www.optus.com.au/portal/site/WOCA/

Standards Australia

Standards Australia is a leading standards development organisation in Australia. Standards Australia strives to enhance Australia's economic efficiency, international competitiveness and the community's expectations for a safe and sustainable environment.

URL: http://www.standards.org.au

TAFE NSW

TAFE New South Wales is Australia's largest educational institution offering more than 1200 courses at more than 130 locations across the state of New South Wales. TAFE NSW delivers study programs and services to meet the needs of students, industry and the community.

URL: http://www.tafensw.edu.au

Telstra

Telstra is a telecommunications and information services company in Australia. Telstra's main activities include the provision of:

- Basic access services to most homes and businesses in Australia;
- Local and long-distance telephone calls in Australia and international calls to and from Australia;
- Mobile telecommunications services; a comprehensive range of data and internet services;
- Management of business customers' IT and/or telecommunications services; wholesale services to other carriers and carriage service providers;
- Advertising, directories and information services; and
- Cable distribution services for FOXTEL's cable subscription television services.

URL: http://www.telstra.com.au

Vodafone

Vodafone provides GSM mobile telecommunications services with network coverage in Sydney, Melbourne, Canberra, Brisbane, Adelaide and Perth.

URL: http://vodafone.com.au

9 APPENDIX C: 17799 MAPPING FOR CISSP, CISA, CISM AND ISSPCS (PRACTITIONER LEVEL)

Introduction

As discussed within the body of this report, there has been considerable discussion around the appropriateness of a single "body of knowledge", and the source of such a body.

Based on feedback during the initial interview process, SIFT presented the following as potential bodies of knowledge to the workshop participants:

- ISO 17799
- AS/NZS 7799.2
- CISSP CBK; and
- NSTISSC 4011.

Discussion led to an understanding that there could be no agreement on a 'body of knowledge' until job skills within information security had been identified.

Similarly, it is acknowledged that to attempt to "map" existing certifications to an information or IT security standard, implies that there is some attempt on the part of those certifications to provide full coverage. As the certifications are primarily based on required job skills, there is no guarantee of a direct mapping to the standards.

Within this context, the following four sections provide mappings of CISSP, CISA, CISM and ISSPCS (Practitioner) to the ISO 17799 standard. As is stated within the report, this is intended primarily to be a point of departure for subsequent efforts to increase the awareness of the programs, and the comparability of the programs.

Certified Information System Security Professional (CISSP)

Summary Analysis

17799 Compliance Map

17799 Compliance Area	CISSP
Security policy	●
Organisational security	◖
Asset classification and control	●
Personnel security	●
Physical and environmental security	●
Comms and operations management	◖
Access control	◖
Systems development and maintenance	●
Business continuity management	●
Compliance	◖

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Functional Roles Map

Functional Role	CISSP
InfoSec Executive (CSO, CIO)	○
InfoSec Operations (ISM)	●
Design & Architecture	◖
Audit	◖
Risk Management	◖
Technical (App)	○
Technical (Network)	○

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Certification Taxonomy

As the first credential accredited by ANSI to ISO Standard 17024:2003 in the field of information security, the Certified Information Systems Security Professional (CISSP) certification provides information security professionals with an objective measure of competence and a globally recognised standard of achievement. The CISSP is a broad-based credential which demonstrates competence in the 10 domains of the (ISC)² CISSP Common Body of Knowledge (CBK).

The (ISC)² CBK is a collection of topics relevant to information security professionals around the world. The (ISC)² CBK establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding.

All members of (ISC)² must abide by the (ISC)² Code of Ethics. There is a formal complaints process for violations against the (ISC)² Code of Ethics.

Body of Knowledge

- Domain 1. Access controls
- Domain 2. Telecom & network security
- Domain 3. Security management
- Domain 4. Applications security
- Domain 5. Cryptography
- Domain 6. Security architecture
- Domain 7. Operations security
- Domain 8. Business continuity planning
- Domain 9. Law, investigations & ethics
- Domain 10. Physical security.

Issuer

The International Information Systems Security Certification Consortium, Inc., or (ISC)^2, is a non-profit organisation, incorporated in the Commonwealth of Massachusetts, based in Palm Harbour, Florida, USA

Goal(s) of the Certification Body

The (ISC)^2 is dedicated to:

- Maintaining the CBK for information security;
- Certifying industry professionals and practitioners under an international standard;
- Providing education;
- Administering certification examinations; and
- Ensuring the continued competence of credential holders.

Business Drivers for Implementing the Certification

People are the key to a secure organisation.

Technology solutions alone cannot protect an organisation's critical information assets. Employers demanding qualified information security staff give their organisations a leading edge by providing the highest standard of security for the information assets of customers, employees, stakeholders and organisations. (ISC)^2 is a non-profit body charged with maintaining, administering and certifying information security professionals via the compendium of industry best practices and the the (ISC)^2 CBK.

Benefits of Certification to the Professional

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

Benefits of Certification to the Enterprise

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

Target Audience

The CISSP credential is ideal for middle and senior level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineers.

Experience Requirements

Applicants must have a minimum of four years of direct full-time security professional work experience in one or more of the 10 domains of the (ISC)^2 CISSP CBK or three years of direct full-time security professional work experience in one or more of the 10 domains of the CISSP CBK with a university degree. Additionally, a Master Degree in Information Security from a National Centre of Excellence can substitute for one year towards the four-year requirement.

CISSP professional experience includes:

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

who simply operates controls under the authority and supervision of others. Titles with the words 'coder' or 'operator' are likely excluded.

Timeliness

The (ISC)² CBK, from which the (ISC)² credentials are drawn, is updated annually by the (ISC)² CBK Committee to reflect the most current and relevant topics required to practise the profession of information security.

Distribution & Examination Methods

Preparation method - Review Seminar

(ISC)² offers seminars that help candidates review and refresh their knowledge of information security. The review seminars are classroom-based events held worldwide on a regular basis. (ISC)²-endorsed seminars are only conducted by instructors authorised by (ISC)². Instructors must be experts in the CISSP CBK domains and remain up to date on the latest information security-related developments.

This CISSP CBK Review Seminar is the only CBK review seminar endorsed by (ISC)².

The (ISC)² CISSP five-day seminar includes:

- Five sessions, each of eight hours duration;
- Post-Seminar Self-Assessment;
- 100 per cent up-to-date material;
- Contributions from CISSPs, (ISC)²-authorised instructors and subject matter experts; and
- An overview of the scope of the information security field.

Delivery of Exam

The examination is seated under the supervision of a local third party partner.

Exam Details

- 250 multiple-choice questions;
- Six hours;
- Pass the CISSP exam with a scaled score of 700 points or greater; and
- Submit a properly completed and executed Endorsement Form.

Identity Verification

Identify is verified by local third party partner.

Re-certification requirements

Upon successfully completing the CISSP examination, the student will receive a certificate and ID card. The student will also be eligible for listing in the CISSP Directory; participation in the Speakers' Bureau; serving on (ISC)² committees and participation in its annual elections.

Re-certification is required every three years, with ongoing requirements to maintain their credentials in good standing. This is primarily accomplished through continuing professional education (CPE), 120 credits of which are required every three years.

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

Number of Holders

As at 1 February 2005:

- 30,681 – Worldwide
- 503 – Australia

Cost

- Early – USD$499
- Standard – USD$599
- Annual CPE maintenance fees of USD$85.

Completeness

The CISSP Common Body of Knowledge has a satisfactory level of detail but does not have full coverage of ISO/IEC 17799 topics. ISO/IEC 17799 areas lacking include:

- 4.2 Security of Third Party Access
- 8.2 System Planning and Acceptance
- 8.5 Network Management
- 9.4 Network Access Control
- 9.5 Operating System Access Control
- 9.6 Application Access Control
- 10.4 Security of System Files
- 12.2 Reviews of Security Policy and Technical Compliance.

Availability

Registration for the CISSP examination is available worldwide.

CERTIFIED INFORMATION SYSTEMS AUDITOR (CISA)

Summary Analysis

17799 Compliance Map

17799 Compliance Area	CISA
Security policy	●
Organisational security	◖
Asset classification and control	◖
Personnel security	◖
Physical and environmental security	◖
Comms and operations management	◖
Access control	◖
Systems development and maintenance	◖
Business continuity management	●
Compliance	◖

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Functional Roles Map

Functional Role	CISA
InfoSec Executive (CSO, CIO)	◖
InfoSec Operations (ISM)	●
Design & Architecture	◖
Audit	●
Risk Management	●
Technical (App)	○
Technical (Network)	○

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Certification Taxonomy

The Certified Information Systems Auditor (CISA) designation is awarded to those individuals with an interest in information systems (IS) auditing, control, and security. CISA contains seven content areas and contains both process and content components in a CISA's job function.

These areas are developed through the job practice analysis of the tasks routinely performed by a CISA and the required knowledge to perform these tasks.

This is a broad-based certification specifically tailored for professionals working in IS auditing, control and security functionalities.

Members of ISACA must abide by the ISACA Code of Professional Ethics. ISACA has a formal process in place for handling complaints against certified members. The CISA certification was accredited by ANSI to ISO Standard 17024:2003 in September 2005.

CISA Content Areas

- Domain 1. Management, Planning, and Organisation of IS
- Domain 2. Technical Infrastructure and Operational Practices
- Domain 3. Protection of Information Assets
- Domain 4. Disaster Recovery and Business Continuity
- Domain 5. Business Application System Development, Acquisition, Implementation, and Maintenance
- Domain 6. Business Process Evaluation and Risk Management
- Domain 7. The IS Audit Process.

Issuer

The Information Systems Audit and Control Association (ISACA), Rolling Meadows, Illinois USA.

Goal(s) of the Certification Body

ISACA is dedicated to serving the needs of its members, who are internal and external auditors, CEOs, CFOs, CIOs, educators, information security and control professionals, students, and IT consultants.

Business Drivers for Implementing the Certification

Since 1978, the CISA program has become a globally accepted standard for IS audit, control and security professionals.

The technical skills and practices that CISA promotes and evaluates are key functional areas within the field. With a growing demand for professionals possessing IS audit, control and security skills, CISA has become a well-regarded certification program by individuals and organisations around the world. CISA certification signifies commitment to serving an organisation and the IS audit, control and security industry. In addition, it presents a number of professional and personal benefits.

Benefits of Certification to the Professional

- Worldwide recognition;
- Professional development opportunities as a large portion of CISAs hold management or consulting positions;
- Certification equips the professional with the knowledge and ability to evaluate:
    1. IS management strategy, policies, standards and procedures;
    2. Effectiveness and efficiency of an organisation's implementation and ongoing management of technical and operational infrastructure;
    3. Logical, environmental and IT infrastructure security;
    4. Continuity of business operations and IS processing;
    5. Business application system development, acquisition, implementation and maintenance;

6. Business systems and processes.

Benefits of Certification to the Enterprise

- Certification demonstrates IT assurance knowledge and skill;
- Certification shows the professional is committed to maintaining skills through future professional development and continuing professional education; and
- Certifies that the professional has acquired professional experience and has passed a rigorous exam.

Target Audience

The CISA certification is designed for professionals who have Information Security Audit, Control and Security functions as part of their job description.

CISA is offered in the following languages: Chinese (Simplified and Traditional), Dutch, English, French, German, Hebrew, Italian, Japanese, Korean and Spanish.

Experience Requirements

A minimum of five years of professional information systems auditing, control or security work experience (as described in the job content areas) is required for certification. Experience must have been gained within the 10-year period preceding the application date for certification or within five years from the date of initially passing the examination. Retaking and passing the examination will be required if the application for certification is not submitted within five years from the passing date of the examination. All experience will be verified independently with employers.

Experience substitutions

Substitutions and waivers of such experience may be obtained as follows:

- A maximum of one year of information systems experience or one year of financial or operational auditing experience can be substituted for one year of information systems auditing, control or security experience;
- 60 to 120 completed university semester credit hours (the equivalent of an associate or bachelor degree) can be substituted for one or two years, respectively, of information systems auditing, control or security experience; and
- Two years as a full-time university instructor in a related field (eg, computer science, accounting, information systems auditing) can be substituted for one year of information systems auditing, control or security experience.

Timeliness

Due to the importance of the job task analysis and the change experienced in the information security profession, the CISA content material will be subject to change beginning in 2006.

Distribution & Examination Methods

Preparation method - Review Seminar

ISACA offers review seminars prior to the scheduled exam periods. Information regarding these seminars is available by contacting the local ISACA chapter or checking the website. (Currently, there are no Australian seminars listed).

Delivery of Exam

The examination is seated under supervision twice a year in December and June.

Exam Details

- 200 multiple-choice questions
- Four hours
- A candidate must score a 75 or higher.

Identity Verification

Identify is verified by a Testing Agency Representative.

Re-certification requirements

In order to become and remain a CISA an individual must agree to comply with the CISA continuing professional education program. This program requires an individual to earn a minimum of 20 hours annually and 120 hours every three years of continuing professional education.

CISA holders must also pay an annual maintenance fee:

- ISACA members: USD $40
- ISACA non-members: USD $60.

Number of Holders

As at March 2005:

- Over 38,000 – Worldwide
- 680 – Oceania.

Cost

- Early – USD$335 (ISACA members), USD$455 (ISACA non-members)
- Standard – USD$385 (ISACA members), USD$505 (ISACA non-members)
- Annual CPE maintenance fees of USD$40 (ISACA members), USD$60 (ISACA non-members).

Completeness

The CISA Domains have a satisfactory level of detail but do not have full coverage of ISO/IEC 17799 topics. ISO/IEC 17799 areas lacking include:

- 5.2 Information Classification
- 6.1 Security in Job Definition and Resourcing
- 7.3 General Controls
- 8.6 Media Handling and Security
- 9.4 Network Access Control
- 9.5 Operating System Access Control
- 9.8 Mobile Computing and Teleworking.

Availability

Registration for the CISA examination is available worldwide.

CERTIFIED INFORMATION SECURITY MANAGER (CISM)

Summary Analysis

17799 Compliance Map

17799 Compliance Area	CISM
Security policy	●
Organisational security	◖
Asset classification and control	●
Personnel security	◖
Physical and environmental security	○
Comms and operations management	◖
Access control	◖
Systems development and maintenance	◖
Business continuity management	●
Compliance	◖

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Functional Roles Map

Functional Role	CISM
InfoSec Executive (CSO, CIO)	●
InfoSec Operations (ISM)	●
Design & Architecture	◖
Audit	○
Risk Management	◖
Technical (App)	○
Technical (Network)	○

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Certification Taxonomy

The Certified Information Security Manager (CISM) certification provides core competencies and international standards of performance that information security managers are expected to master. The CISM credential measures expertise in five information security management job practice areas.

These areas are developed through the job practice analysis of the work performed by information security managers. Thus, CISM is targeted at information security professionals who have acquired three or more years of experience managing the information security function of an enterprise.

This is a broad-based certification specifically tailored for information security managers and executives.

Members of ISACA must abide by the ISACA Code of Professional Ethics. ISACA has a formal process in place for handling complaints against certified members. The CISM certification was accredited by ANSI to ISO Standard 17024:2003 in September 2005.

Information Security Management Job Practice Areas

- Domain 1. Information Security Governance
- Domain 2. Risk Management
- Domain 3. Information Security Program(me) Management
- Domain 4. Information Security Management
- Domain 5. Response Management.

Issuer

The Information Systems Audit and Control Association (ISACA), Rolling Meadows, Illinois USA

Goal(s) of the Certification Body

ISACA is dedicated to serving the needs of its members, who are internal and external auditors, CEOs, CFOs, CIOs, educators, information security and control professionals, students, and IT consultants.

Business Drivers for Implementing the Certification

CISM was developed out of the need for ISACA to serve an increasing number of new and existing members having information security responsibilities. This includes members at all experience levels, including information security directors, managers and consultants responsible for IT governance, risk management and the design and management of information security within their enterprise. Many of these members had earlier earned an information security credential such as a CISA or CISSP and were now in search of a program that would recognise their unique managerial expertise and knowledge. In addition, ISACA identified through research and survey the increased role of the information systems auditor in information security and a trend toward movement later in the IS auditor's career into information security management positions.

CISM's single-minded emphasis is on information security management, through the management focus of its job practice areas and its management experience requirement. CISM's requirement of information security management experience ensures that only those who manage and oversee an enterprise's information security effort can earn it.

Benefits of Certification to the Professional

- Worldwide recognition;
- Professional development opportunities as a large portion of CISMs hold management and consulting positions;
- Individuals earning the CISM certification become part of a large peer network;
- Certification equips the professional with the management ability to:

1. Align information security strategies with business objectives;
2. Identify and manage information security risks to achieve business objectives;
3. Manage an information security program;
4. Oversee and direct information security activities; and
5. Develop and manage a business continuity program.

Benefits of Certification to the Enterprise

- Certification demonstrates information security management knowledge and skill;
- Certification shows commitment to maintaining skills through future professional development and continuing professional education;
- Certifies that the professional has acquired professional experience and has passed a rigorous exam;
- The CISM job practice also defines a global job description for the information security manager and a method to measure existing staff or compare prospective new hires.

Target Audience

- More than 1,000 CISMs serve as a chief information officer, chief executive officer or IS security director;
- More than 2,000 CISMs serve as an information security manager or in a related information security position; and
- Nearly 1,000 CISMs are employed in security consulting or training positions.

Experience Requirements

Submit verified evidence of a 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 substitutions

The following security-related certifications and information systems management experience can be used to satisfy the indicated amount of information security work experience.

Two Years:

- Certified Information Systems Auditor (CISA) in good standing
- Certified Information Systems Security Professional (CISSP) in good standing
- Post-graduate degree in information security or a related field (eg, business administration, information systems, information assurance).

One Year:

- One full year of information systems management experience
- Skill-based security certifications (eg, SANS Global Information Assurance Certification (GIAC), Microsoft Certified Systems Engineer (MCSE), CompTIA Security+).

The experience substitutions will not satisfy any portion of the three-year information security management work experience requirement.

Timeliness

Due to the importance of the job task analysis and the change experienced in the information security profession, ISACA is currently reviewing the job task analysis.

Distribution & Examination Methods

Preparation method - Review Seminar

ISACA offers review seminars prior to the scheduled exam periods. Information regarding these seminars is available by contacting the local ISACA chapter or checking the website. (Currently, there are no Australian seminars listed).

Delivery of Exam

The examination is seated under supervision twice a year in December and June.

Exam Details

- 200 multiple-choice questions
- Four hours
- A candidate must score a 75 or higher.

Identity Verification

Verification is performed by a Testing Agency Representative.

Re-certification requirements

In order to become and remain a CISM an individual must agree to comply with the CISM continuing professional education program. This program requires an individual to earn a minimum of 20 hours annually and 120 hours every three years of continuing professional education.

Number of Holders

As at March 2005:

- Over 5,000 – Worldwide
- 76 – Australia.

Cost

- Early – USD$335 (ISACA members), USD$455 (ISACA non-members)
- Standard – USD$385 (ISACA members), USD$505 (ISACA non-members)
- Annual CPE maintenance fees of USD$40 (ISACA members), USD$60 (ISACA non-members)

Completeness

The CISM Domains have a moderate level of detail but do not have full coverage of ISO/IEC 17799 topics. ISO/IEC 17799 areas lacking include:

- 6.1 Security in Job Definition and Resourcing
- 7.1 Secure Areas
- 7.2 Equipment Security
- 7.3 General Controls
- 8.2 System Planning and Acceptance
- 8.3 Protection Against Malicious Software
- 8.5 Network Management
- 8.6 Media Handling and Security
- 9.2 User Access Management
- 9.3 User Responsibilities
- 9.4 Network Access Control
- 9.5 Operating System Access Control
- 9.8 Mobile Computing and Teleworking
- 10.2 Security in Application Systems
- 10.4 Security of System Files.

Availability

Registration for the CISM examination is available worldwide.

INTERNATIONAL SYSTEMS SECURITY PROFESSIONAL CERTIFICATION SCHEME (ISSPCS) – PRACTITIONER LEVEL

Summary Analysis

17799 Compliance Map

17799 Compliance Area	ISSPCS
Security policy	◖
Organisational security	◖
Asset classification and control	●
Personnel security	◖
Physical and environmental security	◖
Comms and operations management	◖
Access control	○
Systems development and maintenance	◖
Business continuity management	●
Compliance	◖

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Functional Roles Map

Functional Role	ISSPCS
InfoSec Executive (CSO, CIO)	◖
InfoSec Operations (ISM)	◖
Design & Architecture	◖
Audit	●
Risk Management	●
Technical (App)	○
Technical (Network)	○

● - Satisfactory coverage
◖ - Moderate coverage
○ - Minimal or no coverage

Certification Taxonomy

The International Systems Security Professional Certification Scheme (ISSPCS) designation is awarded to those individuals competent in practising Information Security and Security Engineering. The ISSPCS Theoretical and Practical Knowledge Base examines eight Security Process areas in relation to six specific fields of application, called Functional Disciplines.

These areas provide a life-cycle approach to security within an organisation, covering the full range of security related activities from strategic security management to security administration.

This is a broad-based certification for IT security practitioners. The main differentiator between ISSPCS and other certifications is its inclusion of a regionalised component depending on the country of examination. Hhowever, ISSPCS has yet to develop the regionalised components

for examination. The certification is stratified into four levels: ISSPCS Practitioner, ISSPCS Professional, ISSPCS Mentor and ISSPCS Fellow.

Members of ISSPCS are bound by the ISSPCS Code of Ethics. ISSPCS is currently awaiting approval from the Academic Board and ISSEA on the proposed complaints process against ISSPCS members.

ISSPCS Security Process Areas

- 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.

Issuer

The International Systems Security Engineering Association, Herndon, Virginia, USA

Goal(s) of the Certification Body

The ISSPCS developers and ISSEA have striven to develop and implement a professional IT and Systems Security Certification Scheme that has wide credibility and jurisdiction and is genuinely international.

Business Drivers for Implementing the Certification

Presently, organisations are implementing a multitude of enterprise-wide security solutions encompassing people, technology and physical domains in order to deal with the availability, authenticity, integrity, confidentiality and non-repudiation of services. One of the major challenges for the modern organisation is the ability to recognise talent, skills and experience when it comes to the development and implementation of a security regime capable of protecting the organisation's assets. For the security professional, the problem is the lack of certifications available which focus on the general principles of security and their essential foundations.

To address these issues, the ISSEA oversaw the implementation of a global and open certification scheme for security professionals that addresses the shortfalls of traditional IT security certifications by founding the scheme on essential principles of security. The ISSPCS development team is involved in the continual development of the certification program.

Benefits of Certification to the Professional

- Wide credibility, jurisdiction and international;
- The certification is constantly updated throughout the year;
- Vendor-neutral;

- Provides cost-effective certification focusing on the general principles of security and the essential foundations;
- Provides a theoretical and practical base on which to build fundamental skills;
- Addresses the shortfalls of traditional IT security certifications by founding the scheme on essential principles of security;
- Open scheme which is open to all IT and systems security professionals; and
- Various levels of certification may be achieved by successful completion of certified examinations and/or interviews.

Benefits of Certification to the Enterprise

- Ability to recognise talent, skills and experience;
- Credible, comprehensive, cost-effective, international in scope;
- Various levels of the certification offer an indication of professional experience and knowledge;
- Independent scheme with no commercial bias to any vendor or group of vendors;
- The scheme requires the professional to have evidence of continuing development;
- Certification does not simply rely on the regurgitation of a body of knowledge, but is instead founded on demonstrating an ability to apply process and methodology, as well as an understanding of security knowledge and techniques; and
- Scheme is not exclusively IT but also reflects the systems approach, including physical personnel and technological.

Target Audience

The ISSPCS is a four-level program is aimed at developing IT and systems security professionals. The Practitioner examination is the entry level for all applicants.

The ISSPCS program is only conducted in English. Exams are held in Australia, Canada and the US.

Experience Requirements

ISSPCS candidates must have an IT or related degree, and three years of information security experience. The Practitioner certification is valid for three years.

Grandfathering Scheme

Suitably qualified professionals may apply for an ISSPCS Practitioner certification without having to sit or pay for the examination, by utilising the ISSPCS Grandfathering Program. To gain an ISSPCS Practitioner via the Grandfathering Program, the applicant must meet or exceed these requirements:

- Applicant must hold at least one of the following certifications; a current CISSP, CISM, GIAC Security Expert Certification, or SSE-CMM Appraiser Certification;
- Applicant must be able to demonstrate no less than five years of work experience in the information security field;

- Applicant must provide current resume, showing work history that is relevant to the information security or information security engineering fields, and summaries of engagements in information security activities;
- Applicant must provide one personal character reference, written by an associate;
- Applicant must provide one professional reference written by an associate describing their work exposure, work quality and work ethic; and
- Applicant must have successfully completed an ISSPCS Grandfathering Scheme Application, including agreement to uphold the ISSPCS Code of Ethics.

Timeliness

The ISSPCS development team is involved in the continual development of a certification programme that is credible, comprehensive, cost-effective, international in scope, and genuinely open.

Distribution & Examination Methods

Preparation method – Reference Resources

Each ISSPCS level has specific resources that are freely downloadable. There are currently six Practitioner reference resources available.

Delivery of Exam

The examination is seated under supervision, every three to six months.

Exam Details

- Closed book
- Four hours
- A candidate must score 60 per cent or higher

Identity Verification

Candidates must bring current and valid photo identification to the examination venue.

Re-certification requirements

ISSPCS members must achieve a defined number of Activity Points (APs) over the three-year term of their certification. For an ISSPCS Practitioner, 750 APs are required. When the applicant re-certifies, they must have equalled or exceeded the required number of APs for their certification.

Number of Holders

As at March 2005:

- 34 approved from grandfathering, 200 applicants awaiting approval.

Cost

- Standard – AUD$500 / CAD$500 / USD$400
- Triennial recertification fee of AUD$300.

Completeness

The Theoretical and Practical Knowledge Base has an adequate level of detail but does not have full coverage of ISO/IEC 17799 topics. ISO/IEC 17799 areas lacking include:

- 6.3 Responding to Security Incidents and Malfunctions
- 7.1 Secure Areas
- 8.6 Media Handling and Security
- 9.2 User Access Management
- 9.3 User Responsibilities
- 9.4 Network Access Control
- 9.5 Operating System Access Control
- 9.8 Mobile Computing and Teleworking.

Availability

The ISSPCS examination program is currently only available to Australia, Canada and the US.

10 APPENDIX D: BIBLIOGRAPHY

CODE	FULL TITLE; AUTHOR; PUBLISHED DATE; PUBLICATION GROUP
2005	
{AITSF 2005]	*ISIG and AITSF letter to DCITA*; Kaldor, M, Klemm, W; March 2005, ISIG & AITSF
[ANTA 2005]	*National Training Framework (NTF)*; ANTA; 2005 http://www.dest.gov.au/sectors/training_skills/policy_issues_reviews/key_issues/nts/dap/training.htm
[CAEIAE 2005]	Center of Academic Excellence; CAEIAS; 2005 http://www.nsa.gov/ia/academia/caeiae.cfm
[CISSE 2005]	*Education and Certification*; CISSE; 2005 http://www.ncisse.org/certification.htm
[DCITA 2005]	*IT Security Skills Accreditation in Australia: Tender Brief DCON/05/32*; DCITA; May 2005
[Foo 2005]	*Made in Australia security qualification?*; Foo, F; 16 March 2005, ZDNet Australia http://www.builderau.com.au/manage/business/print.htm?TYPE=story&AT=39181121-39024656t-20000989c
[ISACA 2005a]	*2005 CISA Exam Bulletin of Information*; ISACA; 2005 http://www.isaca.org/Template.cfm?Section=Exam_Information&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20382
[ISACA 2005b]	*2005 CISM Exam Bulletin of Information*; ISACA; 2005 http://www.isaca.org/AMTemplate.cfm?Section=CISM_Exam_Info&Template=/ContentManagement/ContentDisplay.cfm&ContentID=20613
[(ISC)² 2005a]	*CISSP Exam Structure*; (ISC)²; 2005 https://www.isc2.org/cgi/content.cgi?category=19%20ISC2.org%20CISSP%20CBK
[(ISC)² 2005b]	*(ISC)² Review Seminar and Examination Pricing*; (ISC)²; 2005 https://www.isc2.org/download/regional_pricing.pdf
[(ISC)² 2005c]	Wake Up and Smell the Mandate! (New certification requirements for US DoD) ; (ISC)²; 2005 https://www.isc2.org/cgi-bin/content.cgi?page=876

[ISIG 2005] *Professional Membership Requirements*; ISIG; 2005
http://www.isig.org.au/Professional%20Membership.htm

[ISSPCS 2005] *About the ISSPCS Practitioner Certification*; ISSPCS; 2005, ISSPCS official website
http://www.isspcs.org/cert/practitioner.php

[ITPC 2005] Infosec Training Paths and Competencies; ITPC; 2005, ITPC official website
http://www.cabinetoffice.gov.uk/infosec/index.asp

[Jenkins 2005] *Industry accreditation moves closer*; Jenkins, C; 15 March 2005, The Australian IT
http://australianit.news.com.au/articles/0,7204,12550458%5E15334%5E%5Enbv%5E15306-15317,00.html

[LeMay 2005a] *Mixed views on AU IT security accreditation*; LeMay, R; 15 March 2005, ZDNet Australia
http://www.zdnet.com.au/news/security/0,2000061744,39184626,00.htm

[LeMay 2005b] *Security group enters accreditation race*; LeMay, R; 5 April 2005, ZDNet Australia
http://www.zdnet.com.au/news/security/0,2000061744,39187091,00.htm

[Mandla 2005] *Certification standards*; Mandla, E; 10 February 2005, ZDNet Australia
http://www.zdnet.com.au/news/security/0,2000061744,39180456,00.htm

[Mullins 2005] *Security certification: What to look out for?*; Mullins, M; 11 March 2005, CNET Asia
http://asia.cnet.com/enterprise/manage/0,39035818,39221122,00.htm

[Parker 2005] *What value your security certification?*; Parker, D; 29 March 2005, The Register
http://www.theregister.co.uk/2005/03/29/security_certification/

[PITAC 2005] *Report to the President – Cyber Security: A Crisis of Prioritization*; President's Information Technology Advisory Committee; February 2005, PITAC
http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

[UKAS 2005] *Certification Body Schedules*; United Kingdom Accreditation Services; 2005
http://www.ukas.com/about_accreditation/accredited_bodies/certification_body_schedules.asp

2004

[ANSI 2004a] *Accredited Personnel Certification Programs*; American National Standards Institute; June 2004

http://public.ansi.org/ansionline/Documents/Conformity%20Assessment/Personnel%20Certifier%20Accreditation/ISO-IEC%2017024%20General%20requirements%20for%20bodies%20operating%20certification%20of%20persons/Client%20Companies%20and%20Applicants/Directory%20of%20Accredited%20Programs-17024.pdf

[ANSI 2004b] *Accredited Personnel Certification Programs-Applicants*; American National Standards Institute; December 2004

http://public.ansi.org/ansionline/Documents/Conformity%20Assessment/Personnel%20Certifier%20Accreditation/ISO-IEC%2017024%20General%20requirements%20for%20bodies%20operating%20certification%20of%20persons/Client%20Companies%20and%20Applicants/Directory%20of%20Applicants-17024.htm

[APEC 2004] *IT Skills Report – APEC*; APEC; 2004, APEC Telecommunications and Information Working Group

http://www.apectel29.gov.hk/download/estg_05.doc

[Fundaburk 2004] *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21st Century*; Fundaburk, A; 2004, Bloomburg University

http://cob.bloomu.edu/afundaburk/personal/The%20Education%20of%20Information%20Security%20Professionals.ppt

[ISIG 2004] *Professional Recognition Update*; ISIG; 20 October 2004, ISIG Website

http://www.isig.org.au/Professional%20Recognition%20Update.htm

[ISPWG 2004] *The Institute for Information Security Professionals – A Blueprint;* Information Security Professionals Working Group; 7 December 2004, Information Security Professionals Working Group

[HKCS 2004] *Commonly Accepted Audit or Assessment Mechanism to Certify Information Security Standards – HKCS Response*; HKCS; 6 October 2004

http://www.hkcs.org.hk/doc_journal/securitybureau.pdf

[Norris 2004] *IT Security Workforce Development and the Role of Professional Certification*; Norris, J. S; March 2004, Federal Information Systems Security Educators Association

[SA 2004] *AS ISO/IEC 17024-2004: Conformity Assessment - General requirements for bodies operating certification of bodies*; Standards Australia; 2004

[Varadharajan 2004] *ICT Security and Certification*; Varadharajan, V; 14 December 2004, Information Age
http://www.infoage.idg.com.au/index.php/id;319104870;fp;16;fpid;0

2003

[Ames, Gaskell & Muir 2003] *Registration and Certification of Information Security Professionals;* Ames, M; Gaskell, G; Muir, M; ISIG Website
http://www.isig.org.au/AusCERT/ISIG%20Discussion%20Paper.htm

[Bogue 2003] *What makes a certification valuable?;* Bogue, R L; 16 June 2003, ZDNet Australia
http://www.zdnet.com.au/jobs/resources/0,2000056675,20275390,00.htm

[Gray 2003] *CISSP security certification under fire from academics*; Gray, P;14 May 2003, ZDNet Australia
http://www.zdnet.com.au/news/security/0,2000061744,20274484,00.htm

[EURIM 2003] *EURIM – IPPR E-Crime Study; Partnership Policing for the Information Society, Working Paper 5: Growing the Necessary Skills*; EURIM; 10 November 2003, EURIM

2002

[IFIP 2002] *TC-11 Statement on Information Security Professionals (Decided during annual meeting on 5 May 2002 in Cairo, Egypt)*

[Jarmin 2002] *ICTSO certification Scheme*; Jarmin, M; 1 October 2002, MAMPU
http://www.ktkm.gov.my/images/ictso.ppt

[Sundt 2002] *Information Security Consultancy – A Study for The Department of Trade and Industry*; Sundt, C; May 2002
http://www.dti.gov.uk/industry_files/pdf/psirep.pdf

2001

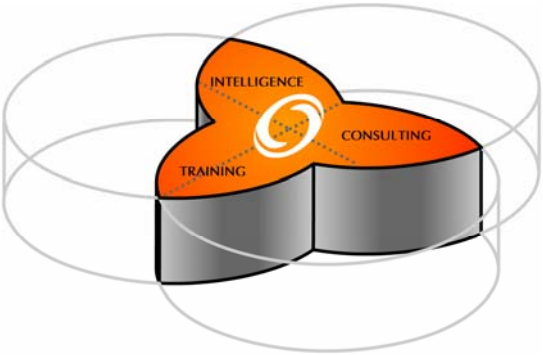
[SA 2001] *AS NZS ISO IEC 17799-2001 Information Technology – Code of practice for information security management*; Standards Australia; 2001

[Wilson 2001] *IN TRAINING: Security courses look for students to fill places*; Wilson, E; 18 September 2001, The Age
http://www2.ma.rmit.edu.au/Kepler/academicstaff/Asha/agearticle.html

1994

[NSTISSI 1994] *NSTISSI No. 4011 – National Training Standard for Information Security (INFOSEC) Professionals*; NSTISS; 1994
http://security.isu.edu/pdf/4011.pdf

SIFT – Our Profile



Founded in 2000, SIFT is a leading Australian pure-play information security consulting, intelligence and training firm. We specialise in the delivery of independent advice, reviews and recommendations to the senior management of large, highly regulated organisations.

Our focussed provision of information security advice and assurance services within the context of industry and country-specific regulatory requirements is unique. Our commitment to our clients is the ongoing delivery of concrete, specific and measured steps across the broad spectrum of information security body of knowledge.

SIFT has built long-term relationships with major clients and information security stakeholders in both the public and private sectors, providing exceptional customer focus throughout our business units. Through our security intelligence and industry and regulatory relationships, we are uniquely positioned to advise on information security within the Australian context.

Also realising the importance of information security in the wider community, SIFT is a sponsor of the Internet Industry Association (IIA) SME security portal, and provides pro-bono consulting services and financial support to The Inspire Foundation & Reachout! – a service that uses the internet to provide much-needed information, assistance and referrals to young people going through tough times.

Our Services

Leveraging our unique perspective of information security issues in the Australian context, SIFT offers its clients a range of services:

Consulting

- Penetration Testing & Risk Assessment
- Information Security Governance, Compliance & Reporting
- Security Reviews, Audits and Benchmarking
- Privacy Strategy & Audit.

Intelligence

- Policy & Procedure Development & Review
- Information Availability & Aggregation Reviews
- Product & Vendor Reviews/Recommendations
- Custom Research Reports.

Training

- Introduction to Encryption & PKI
- Information Security: Tactical Information Control
- Industry-Based Training
- Custom Training Programs.

reachout.com.au

Part of the proceeds from this project will be used to support the work of the Inspire Foundation & **Reach Out!**