2007

Supporting User Evaluation of IT Security Certification Schemes

Nicholas J.A Tate
Deakin University, n.tate@its.uq.edu.au

Sharman Lichtenstein
Deakin University, sharman.lichtenstein@deakin.edu.au

Matthew J. Warren
Deakin University, matthew.warren@deakin.edu.au

Supporting User Evaluation of IT Security Certification Schemes

Nicholas J.A. Tate
Faculty of Science and Technology
Deakin University
Burwood, Australia
Email: n.tate@its.uq.edu.au

Sharman Lichtenstein
School of Information Systems
Deakin University
Burwood, Australia
Email: sharman.lichtenstein@deakin.edu.au

Matthew J. Warren
School of Information Systems
Deakin University
Burwood, Australia
Email: matthew.warren@deakin.edu.au

Abstract

IT Security Certification is an increasingly important qualification for information technology (IT) professionals seeking employment in IT security. Yet currently there is a lack of rigorously developed approaches to support the evaluation and selection by key stakeholders of the most appropriate IT security certification scheme from among hundreds of vendor-neutral and vendor-specific schemes. This paper develops a framework based on categories, characteristics and criteria to support user evaluation and selection of an (IT) Security Certification scheme that satisfies user priorities and requirements. The paper illustrates the use of the framework to support an experienced IT Professional's evaluation. Theoretical and practical implications of the framework and trial evaluation are discussed.

Keywords

IT Security, IT Security Certification, IT Professional, Information Security, IT Certification

Introduction

With current and forecast strong market demand for information security professionals, information technology (IT) professionals are increasingly turning to IT security certification schemes to gain entry to the field. According to IT professionals, IT security certification can improve IT security employability by 1) providing evidence of the possession of key skills and capabilities, 2) garnering greater respect from peers and managers, and 3) affording greater confidence (Whitney 2007). Employers of IT security professionals in the developed world also hold high regard for IT security certification – or higher education (HE) qualifications based on such certification – and consider certification a key selection criterion for recruitment (Hentea & Dhillon 2006).

Despite the growing importance of IT security certification schemes, IT professionals, employers and other stakeholders in IT security certification must decide which IT security certification scheme is "best". Such schemes are developed and offered by national security organisations, higher education institutes and IT vendors. As a result of increasing demand, the number of IT security certification schemes produced by these organisations now ranks in the hundreds. By September 2006, there were around 100 vendor neutral certifications and around 40 vendor-specific certifications (Tittel & Lindros, 2006). From among them, IT professionals, employers, HE institutes and governments evaluate and select a certification. Yet currently, such evaluation and selection relies mainly on piecemeal *ad hoc* non-customised information – for example, the certification survey report of Tittel and Lindros (2006). Such reports take very little account of individual stakeholder preferences and requirements, including national contexts.

We argue that an evaluation and selection process for IT security certification should be based on structured information yielded by a systematic evaluation of candidate certifications. The structured information should reflect stakeholder needs and preferences and should highlight how the candidate certifications compare across a range of key characteristics. A theoretical framework is needed that 1) identifies and organises key certification characteristics, and 2) underpins a systematic evaluation and comparison process by a stakeholder. Such a

framework could also serve to highlight, in the Australian context, whether there is any need for an Australian IT security certification scheme. To the best of our knowledge, no such framework exists in the scholarly or professional literatures.

This paper develops a theoretical framework that, when implemented, will enable user evaluation of IT security certification schemes and help identify a preferred candidate scheme. The framework is intended for use by four key constituent user types – IT professionals, employers, HE institutes and government agencies. The framework is intended to assist a user in understanding and ranking the relative merits and positioning of each scheme, thereby assisting in scheme selection. It may also be used to highlight any emerging need for an Australian scheme. A preliminary framework was developed in an earlier phase of the project (Tate et al 2007). This paper provides a revised framework after conduct of a trial evaluation, and illustrates the framework's usefulness by describing and discussing an experienced Australian IT Professional's trial evaluation of three IT security certification schemes.

We first establish the organisation of the paper. The next section provides a theoretical background that 1) reviews the development of IT security education policy in Australia, 2) reviews existing research in this area, 3) defines objectives for an IT security certification evaluation framework, and 4) synthesises key categories and characteristics for a framework from current literature. After describing the research methodology and design, the paper outlines a framework for the evaluation of IT certification security schemes. Due to paper size constraints, the complete framework (comprising more than ten pages) could not be included here, however Appendix One illustrates a fragment. Next, two sections provide and discuss a trial application of the framework by an experienced Australian IT Professional. Finally, a conclusion section highlights key theoretical and practical contributions arising from the research, identifies future research avenues, and provides final remarks.

Theoretical Background

This section first outlines the development of Australian national electronic security (E-security)/IT security education policy to highlight the significance of this research to Australia. It then reviews previous efforts to categorise IT security certification schemes and highlights the need for a certification evaluation framework. Next, it develops key components for a proposed framework by synthesising relevant literature.

Brief History of Development of Australian E-Security / IT Security Education Policy

In recent years, the (now defunct) Australian National Office of the National Economy (NOIE) supported Australian IT security by undertaking a number of capability projects. NOIE's assigned role was to strengthen Australia's participation in the information economy, and to focus upon key technology issues. The aim of the first NOIE project was to explore Australian "E-security" (as NOIE termed information security) education needs. NOIE identified the main issues as:

- Demand for people with E-security skills was expected to be strong over the next few years;
- Recruitment of personnel with E-security skills was considered difficult compared to other information technology and telecommunications skills;
- The greatest difficulty was found in recruiting people with well-rounded security and risk management skills; and
- Education and training opportunities in E-security were not widely available.

Subsequently, NOIE defined within its national E-security strategy the need for improved education in E-security. According to this strategy, E-security skills were to be taught at Australian universities to all students. Cooperation was sought between Australian universities and industry to teach and develop related courses. However in 2002 the structure and role of NOIE was changed with the consequence that the national E-security strategy was reduced to a feasibility analysis of an industry-backed E-security professional certification scheme, including the potential applicability of such a scheme to Australian industry and government needs.

In April 2004, the Department of Communications, Information Technology and the Arts (DCITA), which had absorbed NOIE, decided to investigate the possibility of an Australian IT security certification scheme. DCITA engaged SIFT which investigated and developed its findings (SIFT, 2005). There was a consensus against developing an independent Australian IT Security Certification Scheme. The principal reasons given were: the anticipated high cost of development and compliance of such a scheme; that existing certification schemes already served Australia well; that legal and regulatory issues in Australia, while differing from those overseas did not require the establishment of a new body of knowledge; and that Australian practitioners sought an internationally recognised scheme. However, the process that the consultants employed to develop the findings involved interviewing a large number of stakeholders and inviting them to a workshop to discuss interim findings and identify the way forward for Australia. Many of these stakeholders were already involved in existing IT certification schemes which may have been adversely affected by the introduction of a new

Australian scheme. It might, therefore, be difficult to refute a charge of bias in the consensus finally reported. In either case, an Australian scheme was regarded as important by several key Australian IT security bodies, and the International Systems Security Professional Certification Scheme (*ISSPCS*) was developed in 2004 by the University of Queensland (UQ), AusCERT and Electronic Warfare Associates, Australia (ISSPCS 2007). It is worth noting at this point that it is possible that the use of a framework for IT security certification evaluation may eventually highlight the need for an Australian scheme such as ISSPCS.

Finally, in May 2007 in the national budget, the Australian Federal Government allocated $13.6 million over four years to improve e-security at a national level, seeking to raise awareness of e-security issues for home users and small businesses including teaching E-security within schools (Coonan 2007). This initiative may, in the future, also address other national IT security issues such as national IT Security education.

Review of Existing Approaches for IT Security Certification Evaluation

Several representative approaches to IT security certification evaluation are here briefly discussed, highlighting their limitations for effective evaluation. APECTEL (2004) provides summary descriptions of five IT security certification schemes, however there is a lack of rationale provided for certification selection. Bean (2004) provides several basic descriptions of five of the main certification programmes however these are highly summarised qualitative descriptions and do not identify characteristics or provide a tabular comparison. Tittel (2003) provides a list of certifications supplemented by a discussion of the differences between vendor-neutral and vendor-specific certifications. However, the list of certifications only provides a name and an estimated level of difficulty, together with general descriptions of the broad programmes. Whitman and Mattord (2003) discuss seven HE programmes and their schemes but mainly provide a broad description of each scheme, mirroring coverage on the various scheme websites. As mentioned earlier, in Australia, SIFT (2005) undertook a review of four major IT security certification schemes to determine whether an Australian scheme should be established. The review concluded there was no need for such a scheme but did not document a comparative table of the characteristics of the schemes examined. It did, however, develop a compliance map for ISO/IEC 17799 and descriptions of the four schemes examined.

Objectives for an IT Security Certification Evaluation Framework

The overarching objective of the proposed IT security certification evaluation framework is to provide a means by which each key stakeholder type can access the most appropriate certification scheme for their requirements. A secondary objective is to allow the Australian Government, and other stakeholders where applicable, to continually review whether there is any need for an IT security certification scheme which specifically addresses the Australian environment (i.e. it is localised for the Australian legal, regulatory and ethical context).

To achieve these objectives will require that the framework comprises a number of independent characteristics that a user could relate to and would consider important. It should also reflect the differing requirements of each stakeholder group, and individuals within groups, through the use of "weightings" in which a stakeholder can "self-select" the characteristics of a scheme that matter most to them.

The framework should also enable an objective pre-population with relevant data about each scheme. Future research will expand on the options for providing such an objective pre-population. It is also likely that a fully fledged tool could be developed that implements the framework, however such a tool is considered beyond the scope of this research.

Elements for an IT Security Certification Evaluation Framework

It is noted that current approaches to the evaluation of IT Security certification schemes, reviewed earlier, do not satisfy the above objectives. Therefore a new framework has been developed by first identifying key elements for such a framework, from relevant literature. First, we identify three key categories and their characteristics. The categories are: *Credibility*, *Accessibility* and *Relevance.*

For a scheme to be accepted by a user, it must be perceived as *Credible* (Facklam, 2002). Three characteristics of credibility are: *governance*, *assessment* and *curriculum definition*. First, if the *governance* of an organisation that offers a particular certification scheme is not open and transparent - with few, if any, conflicts of interest – we argue that the scheme is unlikely to gain sufficient user credibility. In addition, if governance of the scheme is not seen to guarantee its independence from any particular commercial, government or national interests, we argue that the scheme is likely to suffer diminished credibility. The importance of scheme governance is illustrated by the proportion of the ISO 17024 standard - ISO/IEC 17024 (2003) - devoted to the rules for scheme governing bodies. The US Department of Defence requires its personnel to have information assurance certification that is accredited by this standard (McNulty, 2005). Second, the credibility of a certification scheme is linked to its *assessment*. Schultz (2005) suggests that many schemes are too simplistic in their assessment requirements. Third, the IT security *curriculum definition* underpins the body of knowledge for an IT security

professional and is therefore an important credibility characteristic (Hentea & Dhillon, 2006; Schultz, 2005). In particular, the body of knowledge should include discussion and assessment of technological, legal and ethical aspects of IT security (Endicott-Popovsky, 2003). It must also be current and based on relevant international standards.

Accessibility is important for an IT security certification scheme for egalitarian reasons (Bledsoe & Graham 2005). Three characteristics of accessibility are: *access restrictions*, *cost* and *national restrictions*. First, in respect of *access restrictions*, an open certification scheme enables individuals to demonstrate their IT security capabilities, irrespective of training. Access restrictions exist when it is mandatory that a candidate for certification examination first undertake a particular training course, thereby increasing costs and imposing additional constraints. Second, user selection of a certification scheme is likely to be linked to the financial *cost* of access. In the case of international schemes, the notion of affordability varies by economy. It is suggested that a scheme which does not account for such variability is likely to limit user access to the scheme. The increasing importance of all the elements comprising the cost is, as reported in Logan and Clarkson (2005), well illustrated by the practice of determining a Return on Investment (ROI) for the certification. Third, as cybersecurity becomes increasingly important and linked, in the perception of many, to national security, there has been some debate as to whether *national restrictions* should be applied to the selection of candidates for IT security courses. Frincke (2003) observes that "Many security programs already segregate their audiences to a certain extent, for certain material … Some US agencies limit participation to those with US citizenship". In other words, only US citizens may enrol in some IT security courses. An important question is thus: is it possible to have a global IT Security certification scheme if certain aspects of it are limited to citizens of a particular country?

For a scheme to be accepted it must be perceived as *Relevant* by 1) IT security professionals who will seek to be certified under it, 2) the employers who may wish to rely on it for selecting staff, and 3) the national jurisdiction in which it operates. Five key relevance-oriented characteristics are: *vendor neutrality, academic credentials and experience, ethical code, market acceptance* and *localisation*. First, regarding *vendor neutrality*, certification schemes may be differentiated by the providing organisations. There are schemes provided by vendors, which concentrate on certifying that the certification holder has knowledge relating to a particular product from a vendor. There are also schemes which certify broad knowledge of a particular domain, that are generally run by an industry or "not-for-profit" group. Second, regarding *academic credentials and experience*, key questions for a certification scheme are "What are its objectives?" and "How does the scheme relate to an academic degree in IT security?" Experts suggest that vendor-neutral certification is both complementary to, and an extension of, a degree in IT security by generally requiring a degree, a level of experience and some specific knowledge of professional practice in IT security, which would not normally be included in a degree. Vendor-specific certification is generally regarded as not directly linked to either, but rather is linked to skills training for particular equipment. Third, most established professions have adopted an *ethical code*. With IT security, a code of ethics can assume particular importance since the knowledge that is needed to defend systems and networks against attack is the same knowledge that could be used to attack them (Logan & Clarkson 2005). The need for a code of ethics appears to be met by vendor-neutral certification schemes that mandate agreement to their code. Fourth, if a scheme does not gain *market acceptance* from employers and governments, the scheme will lose relevance and use (Claburn 2006). Fifth, *localisation* is important as if a scheme does not account for local variations in law, culture, regulation and market development it is unlikely to be relevant to the jurisdiction where it operates. The APEC IT skill Report (2004) identifies local requirements as key to scheme relevance. It is noted that a number of certifications originate in the USA and, in some cases, their curriculum is based on US legal practice rather than international needs.

Having provided the theoretical foundation for an IT security certification evaluation framework, the next section considers the research methodology and design employed for the research project.

Research Design

The research design comprises four phases. As the environment in which IT security certification evaluation takes place is human-oriented, we elected to use an interpretive research approach (Walsham 1995) to account for the subjectivity and social construction of perceptions. The success or failure of an IT security certification evaluation is significantly dependent on the stakeholders. We therefore sought to understand a range of stakeholder perspectives. As there was no previous rigorous approach to evaluation, we sought an exploratory, multi-method approach.

In Phase One, a literature review was conducted to provide a theoretical background, set framework objectives, and search for existing IT security certification evaluation frameworks, as summarised earlier in this paper. This search revealed only piecemeal approaches that did not systematically consider stakeholder requirements and preferences, and did not meet the key objectives for the framework. Next, as discussed above, scholarly,

professional and popular literatures in the information security domain were reviewed and synthesised to develop key categories and characteristics that underpinned a draft framework.

In Phase Two, the draft framework was explored by a two hour focus group session held at the AusCERT2006 conference on the Gold Coast, Australia, in May 2006. The focus group participants comprised seven senior IT security representatives from industry, HE institutes and national government agencies. Two of the participants are international experts in information security. Three participants are IT security professionals at Australian and New Zealand Universities. The sixth participant is an IT security specialist with a government department, and the remaining participant is the director of IT Security engineering for a major IT vendor. The session was moderated by a senior Australian academic in information security. The focus group session debated significant issues relating to the draft framework. Notes were taken at the focus group, and these, together with a session transcript, were analysed for key themes using iterations of inductive qualitative content analysis. Findings confirmed the current framework and suggested several enhancements. The researcher also further explored those themes that suggested criteria for assessing the framework's characteristics, as follows. He searched literature sources and examined 10 security certifications and was thus able to develop criteria for assessing the framework's characteristics, rationale explaining the inclusion of those criteria, and stakeholder relevance for each criterion. A revised framework was produced incorporating all such findings. This phase is reported in detail in (Tate el al 2007).

In Phase Three the revised framework was trialled by the first author - a senior IT Security Professional – by applying the framework (currently implemented as an Excel spreadsheet for the purpose of trialling) to three IT security certification schemes. The first author has a background which includes work with the ISSPCS scheme which, although significant care has been taken to maintain objectivity, may introduce the perception of potential bias. The aim of this phase was to discover any basic flaws in the process and to identify whether the framework needed refinement. The framework was enhanced as a result of practical difficulties experienced in its implementation.

In Phase Four, recently completed, a confirmatory focus group was held to confirm the framework and identify key challenges and potentialities for implementing the framework as a tool. The results from Phase Four (which confirmed the framework) will be reported in a future publication. This paper reports the key results arising from the first three phases only.

Findings

The main outcome from the first three phases is a framework for IT Security Certification Evaluation, summarised in this section. We also discuss the key findings from the trial assessment.

Framework for IT Security Certification Evaluation

Due to the constraints of paper size, only a fragment (Appendix One) of the complete framework (which is ten pages in total) can be included in this paper. The complete framework is organised by Category, Characteristic and Criterion. There are three categories and eleven characteristics (as described earlier), each of which has several criteria to support characteristic assessment. Also included are rationales that explain the inclusion of criteria in the framework. The complete framework also includes four columns indicating the relevance of each criterion to four key user types - IT Professionals/IT Security Practitioners, potential employers, developers of IT security programs at HE institutes, and Governments determining qualifications for skilled migration purposes. However, the four stakeholder columns are not shown in the fragment in Appendix One for space size reasons. The fragment does, however, include a column for quantitative assessment results and a column for a qualitative assessment results. The use of the two columns in assessment is discussed later. To meet the framework objective where it must reflect user requirements and priorities, there is a column provided for a user-defined weighting in the range 1 – 3, where 1 represents the lowest importance to the user, 2 represents medium importance, and 3 represents high importance. While the rationale explains why a criterion is thought sufficiently important to be included in the framework, it also has the wider purpose of allowing a user to determine the importance to their requirements by the assignation of weightings.

Applying the Framework to a Sample of Three Existing Schemes

The framework was trialled by the first author, using a simple spreadsheet tool based on Excel 2003, in late 2006. The trial assessment was undertaken of a sample of three IT Security Certification Schemes from among the many schemes available. This trial was undertaken by the first author, an experienced senior IT/IT Security Professional. Both quantitative and qualitative assessments were produced as will be discussed. The schemes evaluated are *CISSP*, *CISM* and *ISSPCS*. CISSP and CISM were selected because they are the two schemes which are currently most popular in Australia and ISSPCS was selected because it is the only Australian developed scheme. The Certified Information Systems Security Professional (*CISSP*) certification is offered by

the International Information Systems Security Certification Consortium, or (ISC)². It was founded in 1989 and, according to (ISC2 2007), has been undertaken by over 42,000 information security professionals in more than 110 countries. CISSP is a vendor-neutral scheme that is based on a Common Body of Knowledge (CBK), which is maintained by (ISC)² (ISC2 2007) The Certified Information Security Manager (*CISM*) certification is operated by ISACA. The certification was introduced in 2002 and is aimed at individuals who manage, design and assess Information Security within an enterprise (ISACA 2007). The International Systems Security Professional Certification Scheme (*ISSPCS*) was developed in 2004 by the University of Queensland (UQ), AusCERT and Electronic Warfare Associates, Australia (ISSPCS 2007). It is maintained by UQ and AusCERT and is overseen by an ISSPCS Academic Board under the auspices of the International Systems Security Engineering Association (ISSEA). Although it is the only Australian-developed IT Security Certification Scheme, it is an international scheme, and does not currently have a localised module for Australia, which is why SIFT did not report it as an "Australian" scheme (SIFT 2005).

Trial Quantitative Assessment

A trial quantitative assessment was carried out with the following objectives: 1) to test whether information would be readily available to complete the framework; 2) to determine whether the combination of the questions and the suggested method of quantitative assessment would provide results useful to a comparison of schemes; and 3) to explore whether the use of pictorial representations such as radar diagrams would be helpful in illustrating the differences between schemes. As mentioned earlier, Appendix One provides a fragment of the framework which includes the Quantitative assessment column that provides a suggested method for determining a numerical outcome for each criterion when applied to a particular scheme. It is intended that this is, insofar as is possible, an objective assessment. However, this key point is discussed further later in the paper. It can be seen that in the example characteristic used in the fragment (Appendix One) – *Governance* – each criterion when applied to a scheme will produce an outcome of either 1 or 0; this is the unweighted score for that criterion. A weighted score is obtained by multiplying this score by the user-defined weighting for each criterion and dividing the result by 3 to obtain an outcome in the range: 0 to 1.

To allow a useable number of items for assessment, these scores can then be aggregated by characteristic and category. As an example, to obtain the aggregated score for the governance characteristic, the weighted scores for each criterion are summed and then divided by the number of criteria to - once again - obtain an outcome in the range: 0 to 1. Exactly the same approach is used to obtain aggregated scores for each category. Having obtained aggregated scores for each characteristic and category for each scheme, it is then possible to plot these results as two radar diagrams, one for characteristics and one for categories. Appendix Two illustrates the outcome of this process when applied to the three trial schemes using the trial weighting as determined by the first author. *The reader should note that this is an assessment using the complete ten page framework.* The three diagrams at the top of the page allow a comparison of characteristics and the three diagrams at the bottom of the page are for categories.

In this assessment, it has proved possible to meet the objectives of obtaining the required information for each of the trial schemes and to derive results which support a visual comparison by graphical representation using radar diagrams. A comparison between the trial schemes, using these diagrams, will be discussed later.

Trial Qualitative Assessment

The qualitative assessment is designed to support a more detailed written assessment with which to compare the schemes. A trial qualitative assessment was carried out by the first author on the three schemes, with the following objectives: 1) to provide a user of the framework with a more "in depth" comparative understanding of how each criterion is applied to each scheme; and 2) to provide the user with greater information to support their decision on the weighting to be applied to each criterion. An example of such an assessment for the three schemes, covering part of the Governance characteristic, is shown in Appendix Three with three columns containing the assessments. In each case, it was possible to meet the two objectives by the first author being able to successfully use the assessment to support a decision on weightings. A comparison between trial schemes is discussed below.

Discussion of Trial Assessment

Several important insights were gained as a result of the trial assessment of three IT security certification schemes. First, it became clear that it was feasible, when applying the framework to a group of three sample schemes, to meet all the objectives of the trial quantitative assessment and the trial qualitative assessment.

By reviewing the radar diagrams in Appendix Two, it is possible to identify that for the first author, using his trial weightings for the three trial schemes, the Australian ISSPCS scheme has a closer match to his requirements than do the other two schemes. It is likely that this may be because the author is an experienced

Australian IT Professional and that scheme represents his interests best. In the radar diagrams that compare characteristics, this scheme has both a greater number of characteristics which have reached the maximum value (5 for ISSPCS as opposed to 4 for the other schemes) and, graphically, there is a greater area covered by the connection between points. As can be seen from the diagrams, using these weightings, ISSPCS clearly scores higher than the other two schemes in the areas of credentials/experience, curriculum definition and cost and scores lower only on market acceptance. At the category level, once again ISSPCS is closer to maximum on two of the three points than either of the other schemes and covers a greater area and it can be seen that it scores much higher on credibility and slightly higher on accessibility.

Further, the first author was also able to use the trial qualitative assessment, a fragment of which is shown in Appendix Three, to support the determination of weightings. ISSPCS could, therefore, be judged the most relevant scheme in this comparison, however it must be stressed that this comparison is designed to vary by individual.

Conclusion

This paper has reviewed the development and synthesis of a theoretical framework which provides the foundation for different types of users to compare different IT Security Certification schemes. A fragment of the ten-page framework is provided in Appendix One. The categories and characteristics have their bases in the information security education literature and were confirmed and extended by a focus group of international IT security experts (Phase Two of the project). Criteria and rationale for each characteristic were developed and included in the framework. The ability to employ user-defined weightings for each characteristic was provided, together with a diagrammatic representation of the profile of each certification to allow for a greater level of comparison. The framework has been trialled by its application by an experienced IT security professional to three existing IT security certifications and the results of this trial have been provided and discussed. The development of an automated tool to assist in evaluation and comparison is planned, to be offered via a suitable agency yet to be decided. A confirmatory focus group was recently conducted with very positive results which included the identification of several paths for offering the tool to key stakeholder groups. The findings from the confirmatory focus group will be reported in a future publication.

The framework reported in this paper meets the objectives, outlined earlier, of allowing different categories of users to access the most appropriate certification scheme for their requirements and it would, therefore, enable a potential user of an IT Security Certification to make a more informed choice from the large number of certifications available in the marketplace. It also meets the secondary objective of allowing the Australian Government, and other stakeholders to review whether there is any need for a scheme which specifically addresses the Australian environment (i.e. it is localised for the Australian legal, regulatory and ethical context), by applying the framework with appropriate weighting to the desired local characteristics in order to determine whether any existing schemes meet their needs.

References

APECTEL (2004) IT Skills Report, Asia-Pacific Economic Cooperation Telecommunications & Information Working Group e-Security Task Group, March 2004, URL: http://www.apectelwg.org Document number: telwg29/ESTG/05, Accessed: 7 May 2007.

Bean, M. (2004) The Quest for the IT Security Professional, *Certification Magazine, Nov, 6*(11), p. 46.

Bledsoe, K.L. & Graham, J.A. (2005) The Use of Multiple Evaluation Approaches in Program Evaluation, *American Journal of Evaluation, 26*(3), pp. 302-319.

Claburn, T. (2006) Security Pros get their Due, *Information Week*, 16 January, p. 78.

Coonan, H. (2007) Improving e-security for home users and small business – *Media Release,* May, 2007, URL:

http://www.minister.dcita.gov.au/media/media_releases/improving_e-security_for_home_users_and_small_business, Accessed 11 May, 2007

Endicott-Popovsky, B. (2003) Ethics and Teaching Information Assurance, *IEEE Security & Privacy, Jul/Aug*, pp. 65 – 67.

Facklam, T. (2002) *Certification of Persons – ISO/IEC DIS 17024*, ISO Bulletin, October, pp. 31 – 34.

Frincke, D. (2003) Who Watches the Security Educators? *IEEE Security & Privacy, May/June*, pp. 56 – 58.

Hentea, M. & H.S. Dhillon, H.S., Dhillon, M. & Washington, G. (2006) Towards Changes in Information Security Education, *Journal of Information Technology Education, 5*, pp. 221-223.

Hunsinger, D. S. & Smith, M.A. (2005) Predicting Hiring Managers' Intentions to Use IT Certification in the Selection Process, *Journal of Information Technology Management, XVI*(4), pp. 1-18.

ISACA (2007) CISM, URL:

www.isaca.org/Template.cfm?Section=CISM_Certification&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=16&ContentID=7513, Accessed: 25th May 2007,

ISC2 (2007) CISSP: The International Gold Standard, URL: www.isc2.org/cgi-bin/content.cgi?category=97, Accessed: 25th May 2007,

ISO/IEC 17024 (2003) Conformity Assessment-General requirements for bodies operating certification of persons, International Standards Organisation, pp. 1-10.

ISSPCS (2007) ISSPCS, URL: www.isspcs.org, Accessed: 25th May 2007.

Logan, P.Y. & Clarkson, A. (2005) Teaching Students to Hack: Curriculum Issues in Information Security, ACM SIGCSE Bulletin, in *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education SIGCSE '05*, *37*(1), pp. 157-161.

McNulty, L. (2005) Preparing for Implementation: Professional Certification under DOD Directive 8570.1, in *Proceedings of Military Communications Conference 2005 (MILCOM 2005*), IEEE, *3*, pp.1485- 1487.

Schultz, E. (2005) Infosec Certification: Which way do we turn from here? *Computers & Security*, *24*(8), pp. 587-588.

SIFT (2005) Information Security Skills Accreditation in Australia – The Current State and Industry Consensus on the Way Forward, *SIFT Information Security Services*, November, pp 1-98.

Tate, N., Lichtenstein, S. & Warren, M.J. (2007) Toward User Evaluation of IT Security Certification Schemes: A Preliminary Framework, presented at *IFIP TC-11 WG 11.1 & WG 11.8 Joint Workshop on Fostering Knowledge and Skills for Manageable Information Security*, May 15, Sandton, South Africa, in *Proceedings of IFIP SEC'2007 Conference*, Springer.

Tittel, E. (2003) Security Certification: A Marketplace Overview, Certification Magazine, February, 5(2), pp. SG3-SG6.

Tittel, E. & Lindros, K. (2006) Analysis: The Vendor-neutral Security Certification Landscape, SearchSecurity.com, 26 September 2006.

Walsham, G. (1995) "The Emergence of Interpretivism in IS Research", *Information Systems Research*, *6*(4), pp. 376-394.

Whitman, M. E. & Mattord, H. J. (2003) A Draft Model Curriculum for Programs of Study in Information Security and Assurance, Kennesaw State University, pp. 1 – 83.

Whitney, K. (2007) The International Market for Certification, *CertMag.com*, May.

Appendix 1

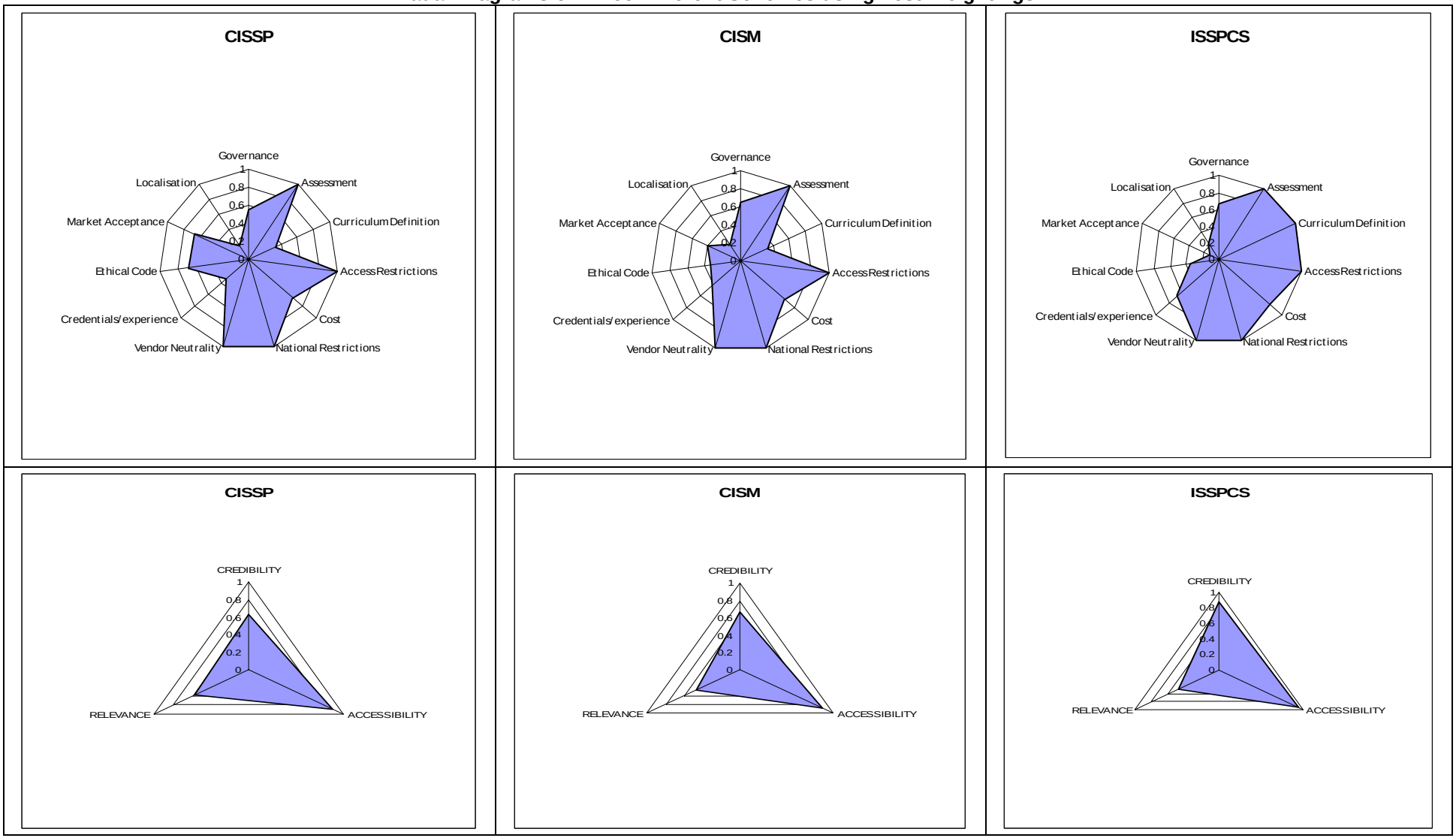
Fragment of Framework with an Example of the Application of Weightings

The table below represents only a fragment of the framework, with an example of weightings applied to the Governance characteristic. **(All weightings are from 1 to 3, with 1 being lowest)**

Category	Characteristic	Criterion	Rationale	A Method of Quantitative Assessment	Qualitative Assessment	Trial Weighting
Credibility	**Governance**	With which governance standards does the CS conform? (e.g. ISO standard 17024?)	If the governance of the organisation which is behind a particular IT security certification scheme is not open and transparent with few, if any, conflicts of interest then the scheme is unlikely to attract the credibility necessary to be successful. The ISO 17024 standard states "The certification body shall be structured so as to give confidence to interested parties in its competence, impartiality and integrity"	No=0 Yes=1		**1**
		Does the CS have a governing Board?	A governing board is the means by which a security CS can demonstrate that decisions are free from the bias of any one individual or organisation.	No=0 Yes=1		**2**
		Is the CS independent of a training provider who may benefit from it commercially or otherwise?	An IT Security CS will be much less credible to all potential users if it is seen to be simply a means of generating more business for a training provider who might own it. Independence from such a provider is, therefore, an important factor.	No=0 Yes=1		**3**
		Are the profits from the CS re-invested in it?	A CS which is operated on a "for profit" basis by its owners is less credible because there is a possible conflict of interest between maximising profits from the scheme and maintaining rigorous standards which are needed for an IT Security CS and which may, for example, reduce the number of people gaining certification.	No=0 Yes=1		**2**
		Is the CS able to operate without direct or indirect government control?	If the governance of the scheme is not seen to guarantee its independence from any particular, government or national interest then the scheme is likely to suffer diminished credibility. In particular, if any one government is seen to exercise control over an IT Security CS then it is unlikely to be readily accepted in other jurisdictions.	No=0 Yes=1		**3**
		Does the governing board of the scheme have members from more than one country?	If all the members of the governing board are from one country, it is likely that the scheme is dominated by the needs of that country and will have much less credibility in other countries. In other words, security certification will be less credible outside the originating country. In particular, there has been criticism of some schemes that they show a strong US bias.	No=0 Yes=1		**3**
		Is the governing board of the scheme able to act independently of the owner of the scheme?	This is a measure of the level of independence of the IT Security CS and the impartiality of the governance process. If the governing board is perceived as being constrained by the interests of the owner then the credibility of the security certification, itself, may be considered compromised.	No=0 Yes=1		**2**

Appendix 2

Radar Diagrams of Three Different Schemes using Test Weightings



Appendix 3

Sample Comparison of the Qualitative Characteristics of Three IT Security Certification Schemes

Evaluation Category	Evaluation Characteristic	Evaluation Criterion	Rationale	Qualitative Assessment CISSP	Qualitative Assessment CISM	Qualitative Assessment ISSPCS
CREDIBILITY	Governance	With which governance standards does the CS conform? (e.g. ISO standard 17024?	If the governance of the organisation which is behind a particular IT security certification scheme is not open and transparent with few, if any, conflicts of interest then the scheme is unlikely to attract the credibility necessary to be successful. The ISO 17024 standard states "The certification body shall be structured so as to give confidence to interested parties in its competence, impartiality and integrity"	ISC2 reports that CISSP complies and this is widely reported	CISM has been accredited by ANSI under ISO 17024	Has not been certified under ISO 17024
		Does the CS have a governing Board?	A governing board is the means by which a security CS can demonstrate that decisions are free from the bias of any one individual or organisation.	There is a publicly acknowledged governing Board	There is a Certification board for CISM, appointed by the board of ISACA, which is the scheme owner.	There is a publicly acknowledged governing board.
		Is the CS independent of a training provider who may benefit from it commercially or otherwise?	An IT Security CS will be much less credible to all potential users if it is seen to be simply a means of generating more business for a training provider who might own it. Independence from such a provider is, therefore, an important factor.	ISC2 organises seminars for CISSP on a "Fee for Service" basis and publishes and markets Scheme reference books	ISACA runs seminars for CISM and produces review documents on a "Fee for Service" basis.	ISSPCS does not directly provide any training

Copyright