Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

AN APPROACH TO VISUALISING INFORMATION SECURITY KNOWLEDGE

Colin James Armstrong

Curtin University,
Perth, Western Australia
Colin.Armstrong@cbs.curtin.edu.au

Abstract. This paper discusses the application of international standards and guidelines together with vendor sponsored accreditation programs in the development of information security curriculum and an approach for visualising that knowledge.

Keywords: ISO27000, COBIT, SFIA, ITIL, information security, curriculum, visualisation.

1 Introduction

Global information communications demand effective and appropriate information security. Teaching information security effectively and appropriately requires incorporating two main dimensions: internationally agreed methods and approaches, and a close organisational fit. Although the majority of organisations have deployed information security capacities, these are not always as effective as organisations would wish. A CSI Survey [1] reports large increases in the incidence of financial fraud, malware infection, denials of service, password sniffing and Web site defacement. In order to better address security management 43% of respondents suffering security incidents changed their organisation's security policy following the abuse [2]. The CISO report published by ISC2 suggests that organisations, like Socrates, need to 'know thyself', being aware of their challenges and opportunities in information systems security management [3]. This report confirms that half of the respondents feel they have a significant ability to impact the security posture of their organisation yet continue to see vulnerabilities and incidents. Emerging new challenges include adoption of social networking applications to improve business processing, and 'cloud' technologies as an alternative repository for corporate information.

Information security curriculum needs to possess the capacity to demonstrate how it addresses these contemporary and other traditional objectives within the much broader encompassing information and communications technology (ICT) arena. Internationally agreed methods and approaches are established through international standards and professional bodies to provide guidance in what to do, how to do it, and who will do it. In the current age of global organisational structure and

ISBN: 1-933510-94-3

communications a baseline is essential in order to determine levels of security management between business partners. When organisations consider venturing into, and extending their business information over the internet, they don't necessarily have the means for quickly and accurately measuring their vulnerability and the risks they offer to other organisations. Compliance with international standards gives some predictability and evidence of compliance provides reassurance that the organisation is probably managing security at an appropriate level for the desired engagement. Business organisations trading in global economic markets require security appropriate to their risk exposure. International standards and guidelines provide the baseline for security requirements and to address these requirements organisations need firstly employees with the essential skills and knowledge and secondly the necessary organisational policies and procedures, to maximise security of their systems. The core body of knowledge recognised by professional associations and certification bodies provides the framework for the necessary skills and knowledge which are delivered by recognised educational institutions. Providing the means of visualising information security subject matter facilitates seeing how well curricula match industry requirements and potential staff capabilities.

Standardising Information Security

The need to ensure information is protected and secure is well established. The roles and tasks performed to secure and protect information communications falls upon those working in the ICT sector. Compliance with expected competencies within this sector is a major undertaking and these competencies should be aligned with internationally agreed standards. There is as yet no clear single agency responsible for overseeing the alignment of internationally agreed standards. The generally accepted core body of knowledge is no longer disputed yet there is a proliferation of organisations offering solutions to the vexed challenge of securing information. Those responsible for managing information security turn to a number of possible solutions. Solutions to securing information focus on what task should be done, how those tasks should be performed, and who is appropriate to perform these tasks. Seeing the relationships between various information security stakeholders and having the means to visualise competencies and capacities associated with information security roles and tasks is also part of the solution.

The ICT stakeholders identified include professional standards organisations, businesses, governments, educators, academic institutions, students, and the community at large. The community at large is a necessary stakeholder because information is exchanged between members of the public and other traditional ICT stakeholders.

Information technology service management relies on professional standards organisations to provide leadership and direction. Professional standards organisations include International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), and special interest groups such as Information Systems Audit and Control Association (ISACA), International Professional Practice

ISBN: 1-933510-94-3 © IFIP TC11.8

Partnership (IP3), and the International Information Systems Security Certification Consortium, Inc. (ISC^2).

One might observe that the ISO/IEC 27000 series and ISACA's CoBIT define 'what' should be done, ITIL defines 'how' it should be done, SFIA defines 'who' should do it, and the various other bodies offer systems of accreditation ensuring 'what', 'how', and 'who' compliance. Two groups; one reflecting the organisation's requirements, the other a practitioner's potential capabilities and the interrelationships between 'what', 'how', and 'who' may be represented, as an information security network as shown in Figure 1.

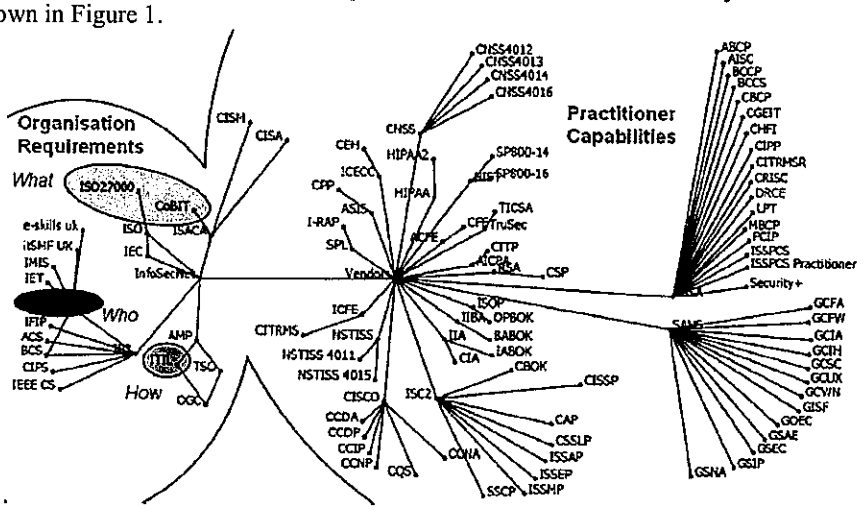

Figure 1: Information Security Network

The ISO/IEC 27000 Series is that most relevant to information security. The comprehensive nature of the ISO/IEC 27000 Series is intended to address every activity considered necessary for managing information security. The generally accepted view is that standards define what must be done and that guidelines explain how to conduct the necessary activities to be compliant with those standards. The Information Systems Audit and Control Association (ISACA) Framework COBIT addresses 'what' should be done by providing technical guidance [4].

How to convert the divergent high level guidance provided by ISO and COBIT into a coherent set of practically implementable tasks suggested in ITL is not obvious. Kulkari [5] discusses the challenges management faces when business processes undergo rapid environmental change and are forced to modify policies to addresses redefined business goals. The COBIT Framework facilitates management of change by addressing the three primary information control topics; security, quality, and fiduciary[6]. Help [7] offers a model of the transition from higher level requirements guidance offered in ISO and COBIT to practical application implementation. The arrangements of the frameworks in Help's model clearly shows the relationship and overlapping between not only each model but also the transitions for 'What' and 'How' in regard to their relationship to standards and guidelines.

ISBN: 1-933510-94-3 © IFIP TC11.8

The Skills Framework for the Information Age (SFIA) is intended to address a perceived lack of agreement on an appropriate framework to describe graduate skills [8]. Organisations employing ICT professionals can use SFIA to write position descriptions, manage risks and improve the ICT function [8]. It has also been used to identify skills attained by graduates of an academic program [9]. The SFIA matrix, that provides skills grouped by categories and subcategories on one axis, while the other axis offers seven levels of responsibility and accountability, is shown as a network in Figure 2. The seven levels are generically described, commencing at the lowest level, as 'Follow' ascending through 'Assist', 'Apply', 'Enable', 'Ensure, advise', to 'Instantiate, influence', culminating at the highest level with 'Set strategy, inspire, mobilise' [10]. Currently, IP3 assumes an ICT professional capacity operating at levels equivalent to SFIA Level 5, and that a university degree program graduate would be able to assume Level 4 responsibilities [10].

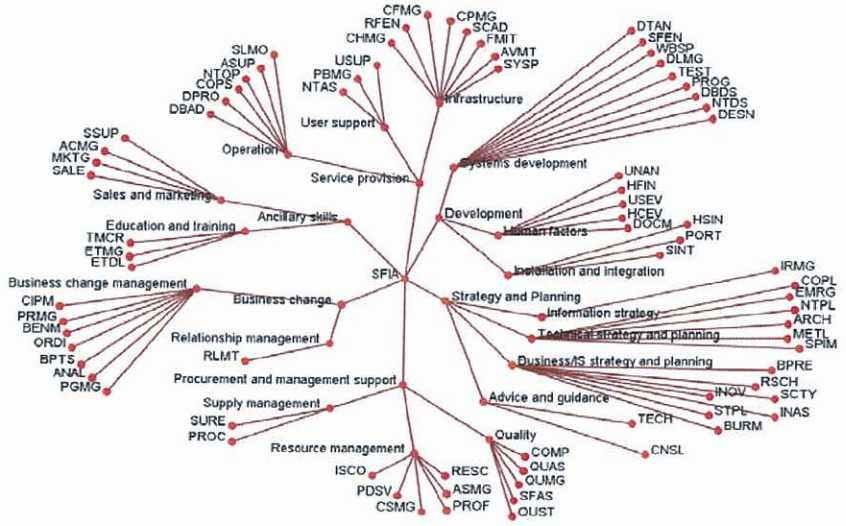

Figure 2: SFIA Skills Network. Adapted from Source: [10].

The crucial issue after determining 'what' should be done is addressing 'how' tasks should be conducted. The Information Technology Infrastructure Library (ITIL) sets out the requisite IT service management concepts and practices for meeting the criteria established in the ISO/IEC 27000 Series and by COBIT. Rudd [11] provides an introductory overview of ITIL explaining the interconnections between ICT management and service delivery, and support mechanisms. Cartlidge et al. [12] furthers Rudd's introductory overview discussing the ITIL service lifecycle in regard to; strategic planning, integrating and aligning business goals, continual improvement, measuring effectiveness and efficiency, optimising costs, achieving a return on investment, developing partnerships and relationships, improving project delivery, outsourcing, gaining a competitive advantage, delivering required services, managing change, and demonstrating governance.

ISBN: 1-933510-94-3 © IFIP TC11.8

Because the primary focus of ITIL is the provision of business IT service, security is sometimes seen as an additional process. ITIL does provide for information security, primarily as a service.

Curriculum Development

The preceding overview shows the nature of contributions to information security curriculum development drawn from the ISO 27000 Series, COBIT, SFIA, and ITIL as used by academic institutions developing course materials. Armstrong and Jayaratna [13] discuss the structure of required information security skills, distinguishing between generic, specialist, and practical skill sets inculcated into a postgraduate internet security management curriculum design. Kim and Surendran [14] offering a Korean perspective discuss four main areas of information security management curriculum design focussing on security policy, risk management, safeguard implementation and training, and safeguard management and conclude with the twelve necessary information security topics.

The Bogolea and Wijekumar [15] survey concluded that curriculum developers should utilise already existing government resources. Armstrong and Armstrong [16] examine alignment of information security education curricula by mapping core body of knowledge and learning outcomes to fifteen national and international accreditation standards. The Theoharidou and Gritzalis [17] review confirms design of academic curricula to conform with CISSP's ten domains meets industry requirements. Dodge, Hay and Nance [18] argue aligning cyber security exercise outcomes assessment to include mapping core body of knowledge in selected standards facilitates measuring student performance.

Examination of core body of knowledge and learning outcomes recommended by academic, government, and vendor publications suggests adopting the CISSP ten domain structure. It is apparent that the core body of knowledge and learning outcomes for information security is well defined. The extent and depth of information to be taught is not disputed but there is a challenge in how best to demonstrate that necessary materials are presented to students and that students have studied the required topics. The apparent lack of a ready means to clearly see the various components of information security is therefore a problem. This problem is not restricted to academia and is exasperated in the business world when non security aware personnel are required to decide organisational requirements, outcomes, and appropriate allocations of resources for meeting information security objectives.

Visualising Information Security Criteria

Information security education and training organisations look to business needs, emerging ICT developments, and build products to sell to those seeking to meet employment opportunities. As pointed out by von Konsky et al. [9], aligning prospective employee capacity, graduate students in particularly, with job criteria is

ISBN: 1-933510-94-3 © IFIP TC11.8

beneficial to both employer and employee. The end objective of curriculum development is graduates succeeding in the workplace. A method facilitating seeing alignments more readily seems a logical next step.

The process for visualising information security curricula alignment to industry standards and guidelines such as SFIA and CISSP learning outcomes, and core bodies of knowledge is modelled in Figure 3. The visualisations are constructed by taking the listed information security categories and attributing them with a value based on the SFIA levels of autonomy and responsibility.

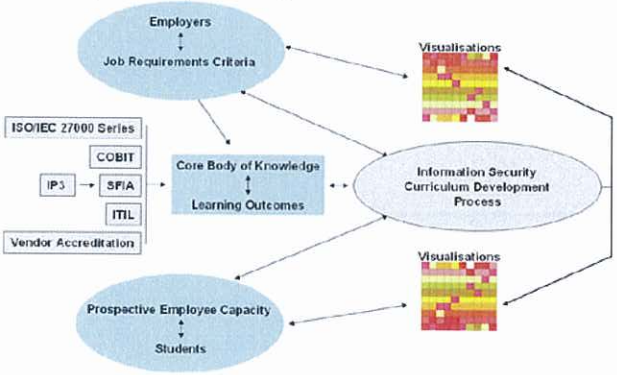

Figure 3: Information Security Curriculum Development Model

A matrix of 78 SFIA categories as shown in Figure 4, each with seven possible levels equates to 546 distinct patterns.

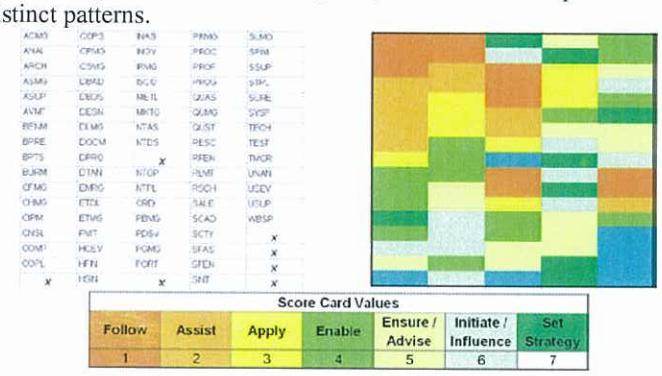

Figure 4: SFIA Coded Matrix Example with Score

Colouring or shading each cell provides an almost unique picture making it a simple matter for the stakeholder, a staff member from human resources department, an academic, or a prospective employee, to develop score card visualisations addressing a set of information security requirements shown in Figure 5.

Figure 5: Example of Required SFIA Skills Compared with Best Available Applicant Skills

Unlike the SFIA framework that provides an alpha code for each skill, the coding used for CISSP relies on a numbering system. This numbering system was derived from the table of contents to CISSP Guide to Security Essentials by Gregory [19]. From the ten chapters, one for each domain, sections and subsections lead to the provision of 78 topics in Chapter 1, 28 topics in Chapter 2, and to eventually provide a total of 680 topics and sub categories.

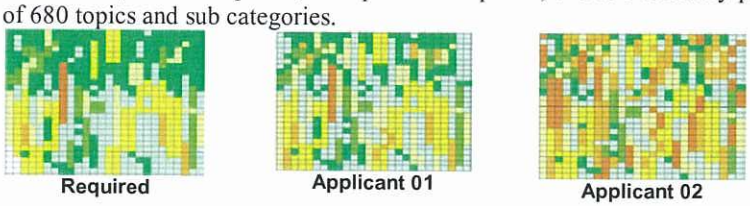

Figure 6: Example of Required CISSP Skills Compared with Best Available Applicant Skills

Conclusion

This paper has provided an overview to some of the influencing factors in the information security curriculum development arena and offered a simple visualisation process for evaluating decision making processes regarding associated skill sets and core knowledge. Adoption of this approach facilitates ready recognition of intricate details to a complex topic independent of external influences. Confirming that this approach using visualisation of information security processes is readily suited to auditing and regulatory compliance purposes is the subject of further current research.

References

1. Peters, S., 2009, 2009 CSI Computer Crime and Security Survey Executive Summary, Computer Security Institute, New York, NY
2. Richardson, R., 2009, 2009 CSI Computer Crime and Security Survey Comprehensive Edition, Computer Security Institute, New York, NY
3. CISO Survey Report, 2010, The 2010 State of Cybersecurity from the Federal CISOs Perspective – An (ISC)2 Report
4. COBIT Framework for IT Governance and Control. Available On-Line @ http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx (20th September 2010)

5. Kulkari M., 2003. Applying COBIT Framework. In Information Systems Control Journal, Vol. 5, Available On-Line @ http://www.isaca.org/Journal/Past-Issues/2003/Volume-5/Pages/Applying-COBIT-Framework1.aspx (20th September 2010)
6. (2008). Aligning COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. A Management Briefing From ITGI and OGC. IT Governance Institute . available On-Line @ http: www.itgi.org
7. Help T., 2008. Case Study: Better to Prevent Than Cure—A New Way to Enhance IT and Business Governance Collaboration. In Information Systems Control Journal, Vol. 4, Available On-Line @ http://www.isaca.org/Journal/Past-Issues/2008/Volume-4/Pages/Case-Study-Better-to-Prevent-Than-Cure-A-New-Way-to-Enhance-IT-and-Business-Governance-Collaboration.aspx (20th September 2010)
8. SFIA (2005) Skills Framework for the Information Age Foundation, 3.0, SFIA Foundation, United Kingdom. URL: http://www.sfia.org.uk/
9. von Konsky, B.R., Hay, D., and Hart, R. (2008): Skill set visualisation for software engineering job positions at varying levels of autonomy and responsibility, 19th Australian Conference on Software Engineering (ASWEC 20008), Industry Experience Report, Perth, 26-28 March, 2008.
10. Gregor, S., von Konsky, B.R., Hart, R., and Wilson, D. (2008). The ICT Profession and the ICT Body of Knowledge (Vers. 5.0), Australian Computer Society, Sydney, Australia.
11. Rudd, C., 2004, An Introductory Overview of ITIL, itSMT Ltd, Earley, UK
12. Cartlidge, A. Hanna, A., Rudd, C., Macfarlane, I,. Windebank, J., and Rance, S., 2007, An Introductory Overview of ITIL® V3. The UK Chapter of the itSMF, UK
13. Armstrong, H. L. and Jayaratna, N. (2002). Internet Security Management: A Joint Postgraduate Curriculum Design. Journal of Information Systems Education, Vol. 13(3).
14. Kim, K-Y. and Ken Surendran, K. (2002) Information Security Management Curriculum Design: A Joint Industry and Academic Effort. Journal of Information Systems Education, Vol. 13(3)
15. Bogolea, B. and Wijekumar, K. (2004). Information Security Curriculum Creation: A Case Study. Published in Conference Proceeding of the 1st Annual Conference on Information Security Curriculum Development. InfoSecCD '04
16. Armstrong, C. J. and Armstrong, H. L. (2007). Mapping Information Security Curricula to Professional Accreditation Standards. "The West Point Workshop", 8th Annual IEEE SMC Information Assurance Workshop, United States Military Academy, West Point, New York.
17. Theoharidou, M. and Gritzalis, D. (2007). Common Body of Knowledge for Information Security. IEEE Security & Privacy. March/April 2007, vol. 5 no. 2
18. Dodge, R. C. Hay, B, and Nance, K. (2009). Standards-Based Cyber Exercises. International Conference on Availability, Reliability and Security, ares, pp.738-743, 2009
19. Gregory, P. H. (2009) CISSP Guide to Security Essentials. Cengage Learning, Boston USA

ISBN: 1-933510-94-3 © IFIP TC11.8