2008

Mapping Information Security Standards: A Counter-Terrorism Example

Gail Ridley
University of Tasmania, Gail.Ridley@utas.edu.au

Jacky Hartnett
University of Tasmania, j.hartnett@utas.edu.au

Wilumpa Jarern-iamsakul
University of Tasmania, wilumpa.jarerniamsakul@utas.edu.au

MAPPING INFORMATION SECURITY STANDARDS: A COUNTER-TERRORISM EXAMPLE

Ridley, Gail, School of Accounting and Corporate Governance, University of Tasmania, Private Bag 86, Sandy Bay, Tasmania 7001, Australia, gail.ridley@utas.edu.au

Hartnett, Jacky, School of Computing and Information Systems, University of Tasmania, Locked Bag 1359, Launceston, Tasmania 7250, Australia, j.hartnett@utas.edu.au

Jarern-iamsakul, Wilumpa, School of Accounting and Corporate Governance, University of Tasmania, Private Bag 86, Sandy Bay, Tasmania 7001, Australia, wilumpa.jarerniamsakul@utas.edu.au

Abstract

Although practitioners have mapped the alignment between IT-related standards, this work has rarely been reported in the academic literature. In particular the methods used have not been made explicit, which has limited the value of any reported results. The research described in this paper demonstrates a rigorous method for mapping the alignment between two example IT security standards. The two standards were Control Objectives for Information and Related Technology (COBIT), widely used as a comprehensive IT control framework, and the Australian Government Information and Communications Technology Security Manual (ACSI 33) which sets out policies and procedures for IT security for Australian government agencies. Conceptual analysis was used to analyse the alignment between the two standards to reveal some insightful patterns of use and emphasis. As one of the security standards defines the base level ICT security for Australian government agencies, related future work using conceptual analysis has the potential to contribute to improved evaluation of the preparedness of commercial Australian organisations to protect the security of their systems from terrorist activities. This paper illustrates the value of such work within a counter-terrorist setting, where leverage for systems security compliance can be gained from voluntary adoption of a commercial standard.

Keywords: COBIT, ACSI 33, Systems security, Content analysis, Counter-terrorism.

1 INTRODUCTION

It is now impossible for organisations to manage without information systems (Ahlgren, Breidne and Hector 2005, Brooks, Warren and Hutchinson 2002). However, the benefits that information systems bring to organisations are also accompanied by risks (Hale and Brusil 2004). Information security was the leading concern about technology in 2007 (The American Institute of Certified Public Accountants (AICPA) 2007). The AICPA views information security as the hardware, software procedures and processes in an organisation that are designed to protect its information systems from both external and internal threats. Information assurance is a process to ensure that the desired information security goals for an organisation are achieved. Risk analysis aims to reduce the vulnerabilities that impact on computer systems in organisations, which may vary from hardware and software issues, to those that deal with human resources and business issues (Brooks et al. 2002). The same vulnerabilities may also threaten national security, as "…increasing dependence upon telecommunications and information infrastructures puts at risk the economic, political and military security of the free world" (Romero 2005, p. 101).

Although many approaches have been taken to security risk analysis, one approach is to develop and implement "minimally acceptable security countermeasures" (Brooks et al.) 2002, p. 377. One such countermeasure is the use of Information Systems (IS) security standards in organisations, which are often referred to as Information Technology (IT) security standards. Because different organisations use different IT security standards, and some use more than one standard of this type, it is useful to understand the differences and commonalities between these standards. Consequently, there has been considerable interest recently in mapping IT standards in the practitioner literature, particularly IT security standards. One example of this work is the mapping of COBIT and ISO 17799 (27002) (ITGI 2000). A strong motivation for this work is to determine the degree of compliance with one IT security standard when implementing another.

Even though many practitioner studies have mapped a range of IT security standards against others, little if any explanation of the methods used has been provided in such work, which limits the confidence of academics in the findings. Furthermore, almost no academic studies have been published that consider the alignment between IT security and other standards. The study reported upon in this paper aimed to identify a scholarly method for mapping the alignment between IT security-related standards. The method is implemented using two IT security-related standards, the *Australian Government Information and Communications Technology Security Manual* (ACSI 33) and the information assurance aspects of *The Control Objectives for Information and related Technology* (COBIT) as examples. To demonstrate the potential value of undertaking research that maps IT security standards, this study is set within a counter-terrorism context. However, a range of other IT security standards could be mapped using the method, which would not necessarily have a counter-terrorism setting.

ACSI 33 is a baseline IT security standard which has been developed by the Defence Signals Directorate (DSD) of the Australian Department of Defence. ACSI 33 provides guidance to Australian Government departments, agencies and commercial service providers on minimum standards for their information and communication technology (ICT) security (DSD 2006). ACSI 33 is designed to strengthen the security of sensitive data and systems used by government agencies, in part, to counter terrorist ICT activity. Many, but not all, of the standards set out in ACSI 33 are mandatory for the organisations to which they apply. COBIT is a standard that includes IT security issues but focuses on the alignment between the use of IT (and hence IT security) and the achievement of organisational business goals. Numerous organisations have adopted COBIT, even though there may be no requirement for them to do so, in order to access the commercial benefits that accompany its effective implementation.

2 BACKGROUND

2.1 Counter-terrorism and IT security

There are two ways in which the security of nations is dependent on ICT. Romero (2005) reports that first, the ongoing delivery of goods and services to sustain the economy, trade and the military, is critical for national security. These goods and services arise from activities that include manufacturing, governing, banking and finance, all of which rely on ICT. Second, critical infrastructures like power, telecommunication, transport, banking and finance are also dependent upon ICT (Romero 2005). Any one of these critical activities could be disrupted by a terrorist attack on a nation's ICT.

The inter-relatedness of national information infrastructures for the public and private sectors is of concern (Ahlgren et al. 2005). As an example, in the United States of America (US) the bulk of the telecommunications section of the national information infrastructure is provided by commercial providers (Andrews 1996). Consequently, some aspects of national security depend upon the security of computer systems of commercial organisations. This characteristic is one reason why governments take an interest in the information security of commercial organisations, particularly as numerous security threats to the computer systems of commercial organisations have been widely acknowledged. The US Department of Homeland Security called for cooperation among government, academics and private industry to reduce vulnerability for information security (Hawkins, Alhhajjaj and Kelly 2003). One way to reduce the security risk arising from ICT dependence is to adopt ICT security standards.

2.2 Baseline security standards

Information security standards are published by organisations for a variety of audiences. A diversity in level and granularity of information security standards reflects an essential problem with security standards. Although the security best practice for a specific piece of ICT infrastructure may be sought, the answer is likely to depend upon the relevant current security goals, which will have been arrived at by organisational processes at a much higher level.

Some security standards are overtly about technology. These standards are published so that vendors and purchasers of ICT equipment can be sure that the specified security functionality is present and performs to the stated specification level. Such standards conform to a more traditional idea of standards; statements against which evaluation can take place. The Trusted Computer Security Evaluation Criteria (DoD 1985) was the first of such criteria. The European Information Technology Security Evaluation Criteria (ITSEC Working Group, 1991) brought together expertise and experiences to define a set of criteria still in use today. This use of international expertise to produce combined international evaluation standards is reflected in the Common Criteria (Common Criteria Editorial Board 1998) which incorporate experiences and work from Canada, the European ITSEC community and the US. It is these evaluation criteria that are most commonly referred to in technology specific standards. Phrases such as 'Agencies should select products from the Evaluated Products List' (ACSI 33, p3–21) are typically found in more general standards.

Management level security standards have also converged to become international standards adopted as national standards. ISO/IEC 1779:2005 is adopted in Australia and New Zealand as AS/NZS ISO/IEC 1779:2006 while the British Standard, BS 7799 is now an international standard, ISO/IEC 270001. An important feature of both these standards is their focus on first defining the desired security goals for an organisation. Emphasis is placed on risk analysis as an essential pre-requisite to defining security requirements and selecting controls. Essentially however, the standards are about suggested controls for implementing and managing ICT security, and are guidelines for best practice.

ACSI 33 is a security standard that is designed to ensure that the ICT systems of Australian government agencies are appropriately protected (DSD, 2007); it is updated each year. ACSI 33 reflects a similar history to other security standards. Although it was originally designed for IT specialists (Brooks et al. 2002), consistent with the need for ICT security risk analysis to consider a broad range of issues, it has evolved to include user training and awareness, the ICT product lifecycle and ICT security roles and responsibilities. ACSI 33 makes extensive use of the terms, MUST, SHOULD and RECOMMEND to guide its intended audience on the level of compliance required. It is divided into three parts, with chapters within each section devoted to particular topics.

COBIT is not specifically a security standard and therefore differs in its scope and purpose to ACSI 33. COBIT is an internationally accepted control framework for IT that facilitates managers to bridge the gap relevant to control requirements, technical issues and business risks. However, as it is designed to be comprehensive, it includes IT security controls. COBIT consists of IT processes that can be categorised into four major domains: *Plan and Organise* (PO), *Acquire and Implement* (AI), *Deliver and Support* (DS), and *Monitor and Evaluate* (ME). The domains are intended to broadly parallel the phases of the systems development life cycle. An IT process is a:

> …collection of IT-oriented procedures influenced by the organisation's policies and procedures that takes inputs from a number of sources, including other processes, manipulates the inputs, and produces outputs, including other processes (IT Governance Institute 2007, p.192).

Each of COBIT's IT processes, and the lower level control objectives associated with each IT process, has a code that indicates the domain from which it comes. For example, the IT process DS5 belongs to the *Deliver and Support* domain. A control objective states the desired result or purpose to be achieved by implementing control objectives in a process (IT Governance Institute 2007, p.190).

Efforts to comply with the US Sarbanes-Oxley (SOX) Act of 2002 (Brown and Nasuti 2005) by adopting COBIT provides much of the explanation for COBIT's burgeoning international popularity. Internal control assertions after the introduction of SOX changed from being largely voluntary, to being based on the Internal Control Integrated Framework from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (Damianides 2005). COSO is a control framework that is used around the world for financial reporting, and has influenced COBIT.

It can seen that there is a tension between those Information Security (IS) security standards that focus on technology alone, and those that acknowledge that security is driven by organisational goals. The latter standards have been associated with a growing interest in security governance.

2.3 Security governance

Even though information security is not only a technical issue, often organisations deal with it in this way (Connor and Coviello 2004). Ahlgren et al. (2005) report that only around 10% of information security is about technology. If this figure is even approximately accurate, the need to go beyond technical issues when dealing with information security is compelling.

Information security is also a business and governance issue. As information security involves risk management, reporting and accountability "…(t)he road to …(it) goes through corporate governance", where corporate governance is the "…set of policies and internal controls by which organisations…are directed and managed" (Connor et al. 2004, p. 5). Therefore, for security to be effective, an organisation's information security governance needs to be embedded into its corporate governance and is closely related to its IT governance. Consequently, information security will be an integral component of organisational operations, requiring the engagement of executive management (Connor et al. 2004). It can be seen that security governance is an organisational issue that needs to consider "people, business processes, infrastructure, applications, information and facilities" (Allen 2006, p. 3).

Best-in-class organisations consider a broad range of issues to address their security, in addition to technology, including their structure, strategy, processes and metrics (Hurley 2005). That is, best-in-class organisations practice security governance. There is evidence that organisations that are most effective at security governance achieve advantages that include reduced risk, and increased customer confidence, cost savings and profit, while accelerating information flow between and among customers, business partners, suppliers and employees (Hurley 2005). These benefits motivate organisations to improve their governance of IT security issues.

2.4 Leveraging systems security compliance from use of commercial standards

The United States (US) Corporate Governance Task Force has recommended that the US Department of Homeland Security should encourage private sector organisations to integrate cyber security within their corporate governance strategies (Connor et al. 2004). The same authors also proposed that the IT controls of organisations need more attention, and called for revision of COSO to include information security governance. As COBIT has drawn upon COSO in its development, the US Corporate Task Force suggested that COBIT and ISO 17799 (27002) be used by organisations to guide their governance of information security (Connor et al. 2004). However, the US Corporate Task Force has stated that information security governance to strengthen cyber security is most effectively achieved voluntarily, rather than being mandated by government (Connor et al. 2004). Therefore voluntary adoption of COBIT by commercial organisations is more likely to be effective for improved information security than enforcing compliance with a standard like ACSI 33.

The research reported upon in this paper aimed in part to investigate whether is was feasible to identify the alignment between COBIT's information security objectives with ACSI 33. Determining this feasibility has the potential to reveal the degree to which commercially-driven implementation of COBIT will also satisfy compliance with the systems security goals of ACSI 33. Such results have the potential to allow leveraging from the voluntary adoption of COBIT by organisations for the commercial benefits it brings, to enable greater awareness and monitoring by the Australian government of the ICT security practices of commercial (and also public) organisations. For example, as stated earlier the critical infrastructure of many nations is controlled by private enterprise to a large degree. Understanding the commonality and differences between a commercially driven standard used for IT security like COBIT and a national government IT security standard (like ACSI 33) could help inform government of the degree to which private enterprise organisations comply with a national government IT security standard when adopting a commercial IT standard. This understanding may contribute to improved evaluation by government of the preparedness of Australian commercial organisations to protect the security of their IT systems from terrorist activities.

Further, as many IT security standards exist and they have different goals, as was discussed in Section 2.2, there will be a need to compare these standards for coverage and emphasis. Therefore the investigation also sought a method for investigating the alignment between two standards that address security that could be justified for an academic audience, as there appear to be almost no academically-focussed publications that have done so. While this method will be demonstrated through comparison of the information assurance aspects of COBIT and ACSI 33, other security standards could be chosen for the mapping process, such as ISO27001 and the IT Infrastructure Library (ITIL). The identification and utilisation of a method for mapping one ICT security standard to another, while retaining academic rigour, will in itself make a contribution to the literature.

3 METHODOLOGY

3.1 Content analysis

Content analysis is a quantitative, systematic research method that determines an occurrence of key words or concepts in texts or other forms of communication (Busch et al., 2005; Carley, 1993). Content analysis is used in policy analysis (Jauch *et al*, 1980) to examine the level of compliance with laws, rules, policies and procedures, as well as to evaluate the alignment between the activities and the goals, objectives and strategies stated in the policy (Texas State Auditor's Office, 1995). However, in the information security academic literature, content analysis appears to be a novel method. This is possibly because content analysis has been used mainly in the social sciences and humanities, while those working in the information security area are more likely to have a background from the sciences. From a search of relevant scholarly literature only one application of content analysis to the security area was identified. In that publication information security threats, controls and standards were analysed to identify generic components of malicious software (Brooks et al. 2002). However, in common with practitioner studies to map IT standards, little explanation of the process of applying content analysis was provided in this study.

Two main types of content analysis exist. The first is *Conceptual Analysis*, which focuses on the occurrence or frequencies of concepts that are usually described by words or phrases in the text. The second is *Relational Analysis*, in which the relationship among concepts in the text is examined (Busch *et al*., 2005). As the aim of the investigation was to explore mapping the information assurance concepts from ACSI 33 to those in COBIT, the focus was on determining the occurrence and frequency of common concepts, rather than to evaluate the relationship among the concepts. Consequently, conceptual analysis was adopted for the current investigation.

A number of limitations in undertaking content analysis has been acknowledged. Unless the process is repeatable, the method is seen as subjective and lacking in rigour. Therefore a critical step in undertaking content analysis is to examine inter-coder reliability (often referred to as inter-coder agreement) which measures the agreement between two or more coders, disregarding the agreement by chance. As another approach to reduce subjectivity, methodologies have been developed for undertaking content analysis consistently, for example, the process developed by Carley (1993). A particular difficulty in mapping standards has been acknowledged, associated with different levels and granularity of some standards when compared to others. For example, some standards like COBIT are at a higher level than detailed procedures of other standards, like ISO.IEC 17799 (27002):2005. The method developed for mapping needs to be capable of accommodating such differences.

3.2 Procedure and analysis

Carley's (1993) method for content analysis was followed by two researchers trained in the technique, with prior experience at mapping standards, including mapping using COBIT. The eight-step procedure followed is set out in Table 1 below, along with a discussion of the application of each phase to the current research project.

Before Step 1 commenced, the researchers selected the documentation for analysis to identify key concepts, to be used in the mapping process. This preliminary step involved selecting the versions of ACSI 33 (unclassified September 2006 version) and COBIT (version 4.1) to be used for analysis, and then identifying the information assurance concepts in ACSI 33 for mapping to COBIT 4.1. Only Parts 2 and 3 of ACSI 33 were considered, as the content of Part 1 was repeated in the other two parts.

Agreement was reached with the Defence Signals Directorate on the definition of Information Assurance, and its source, to be used for analysis during the project.

Step no.	**Application to current project**
1. Decide the level of analysis *(whether to code for a single word or sets of words or phrases)*	Word or phrases were coded to capture broad-based concepts
2. Decide how many concepts to code for *(whether to use predefined or interactive concept choices)*	A list of concepts was developed incrementally during the coding process as it allowed more complete coding of all the concepts that appeared in the text
3. Decide whether to code for existence or frequency of a concept *(answer the question: Am I going to code for existence or frequency?)*	Coding both for existence and frequency was undertaken. Coding for existence aimed to identify the key information assurance concepts presented in ACSI 33 and to examine whether these concepts also appeared in COBIT. Coding for frequency allowed the most strongly aligned concepts to be identified.
4. Decide on how to distinguish among concepts *(whether concepts are coded as they appear or as the same even if they occur in a different form)*	Concepts were coded as the same even when they appeared in different forms. Eg, while coding *"Hardware destruction"*, other sets of words with the same or similar meanings were recorded as matched concepts, *including "Agencies [MUST] destroy unsanitised classified media…"*, and *"To destroy media, agencies [MUST]…"*. This step helped accommodate differences in the levels and styles of the standards referred to as a limitation of the method.
5. Developing rules for coding texts *(create translation rules to allow the researcher to control & organise the coding processes)*	A thesaurus of terms for related concepts from the text, to be used for analysis, was compiled. Examples of the translation rules used are shown in Table 2.
6. Decide how to deal with non-relevant information *(whether to ignore/reanalyse/modify the coding rules)*	Non-relevant information in both ACSI 33 and COBIT was discarded.
7. Coding the text *(undertake textual coding, using manual methods or automated software)*	Analysis and classification were done manually; it was not possible to classify accurately the implicit textual characteristics using software.
8. Analysis of results (*including inter-coder reliability*)	To reduce subjectivity, a reliability co-efficient was sought within range, 0.7–0.9, from independent coding of sample by second researcher; results of mapping analysis presented as frequencies in tables and figures.

Table 1. Content analysis phases followed, and application to the investigation (adapted from Carley 2003).

ACSI 33 concepts for software security	**Rules (look for any word or sets of words that…)**
ICT Security Plan	Demonstrates the development & deployment of ICT security plan and procedures
Security Requirements for Software Development	Demonstrates the procedures that ensure the security of software development
Software Security Requirements for Email	Demonstrates the procedures used to ensure that email is securely used (and/or) managed within the organisation
Software Security Requirements for Malicious Code and Anti-Virus Software	Demonstrates the procedures used to ensure that malicious code and anti-virus software is properly and securely used and managed within the organisation

Table 2. Examples of translation rules used in analysis to derive thesaurus (Phase 5).

The analysis, results and discussion after mapping the information assurance elements of COBIT to ACSI 33 are presented in the following section.

4 ANALYSIS, RESULTS AND DISCUSSION

The final step of Carley's (1993) process for content analysis required evaluation of inter-coder reliability, and undertaking analysis to examine the alignment of the two standards. Analysis of inter-coder reliability fell within the accepted range, when two independent methods were used to measure inter-coder agreement. Example results of analysis of the alignment of COBIT 4.1 and ACSI 33 are provided below, presented as frequencies in tables and a figure, with discussion, to demonstrate application of the method and its potential.

4.1 Information assurance concepts by domain and IT process

As COBIT is designed to cover more than information assurance, and ACSI 33 is largely about information assurance, identifying the COBIT components that dealt with information assurance was a broad way of revealing the commonality between the two standards. By applying the method it was possible to identify information assurance concepts in 26 of COBIT's 34 IT processes, spread across all four domains, as seen in Table 3.

COBIT domain	**No. of IT processes containing info assurance**	**Total no. of IT processes in COBIT**
Plan and Organise (PO)	8	10
Acquire and Implement (AI)	6	7
Deliver and Support (DS)	9	13
Monitor and Evaluate (ME)	3	4

Table 3. Domains and IT processes in COBIT containing information assurance concepts.

The results indicate that COBIT is concerned with information assurance to a considerable extent, and suggest that despite differences in the nature of the two example IT security-related standards to be mapped, it will be possible to map the alignment between ACSI 33 and the information assurance aspects of COBIT. This finding also suggests that by adopting COBIT, organisations will be likely to at least partly comply with ACSI 33. So therefore, for example, if private enterprise critical infrastructure organisations adopt COBIT, and the extent of the adoption is known, the results of this mapping process could inform the Australian Government of the degree of their compliance with ACSI 33. Consequently, the Australian Government will also better understand the preparedness of those organisations' ICT systems to be resilient under terrorist attack.

4.2 Mapping of information assurance concepts by control objectives

Next, analysis was undertaken of the alignment between each of the four domains from COBIT and ACSI 33, working at the chapter level of ACSI 33.

Using the method, the key concepts were identified, and a thesaurus of equivalent terms found was developed for each concept as the mapping progressed. The method revealed the frequency in alignment between COBIT and each ACSI 33 chapter. In this study the greatest alignment was found in COBIT's *Deliver and Support* domain. The method also allowed the researchers to drill down into COBIT at the control objective level. In our study the three IT processes, *Define the IT Processes, Organisation and Relationships* PO4 *(*with 12 control objectives), *Ensure Continuous Service* DS4 (10) and *Ensure Systems Security* DS5 (11) were found to have the greatest number of control objectives containing information assurance concepts. Table 4 displays a summary of the results, with the frequency of COBIT's control objectives containing information assurance concepts in the four domains, which were mapped to each chapter of ACSI 33.

Table 4 suggests that the method used is able to identify data patterns between two IT security standards. For example, the frequency of mapped control objectives from ACSI 33 to COBIT was

much higher for Part 3 of ACSI 33 on *Security Standards* (with 531) than for Part 2 on *ICT Security Administration* (with 224). This finding suggests that the two example IT standards considered had greater common ground for security standards than for the administration of security issues. The method allows these global patterns, and others, to be revealed. As another example, the frequency of alignment between the control objectives of COBIT and individual ACSI 33 chapters ranged from four, for Chapter 5 of Part 2, *Developing a Systems Security Plan (SSP)*, to 109 for Chapter 5 of Part 3 on *Software Security*, which again suggests more alignment between the example IT standards for technical security issues than for organisational or governance issues. These results suggest the areas where the ICT systems of COBIT-adopting organisations will be strongest and weakest when encountering terrorist attack. In general, high frequency counts for components of ACSI 33 found in COBIT suggest closest alignment. However, the frequencies of each concept from each ACSI chapter need to be examined further, as a high frequency may have arisen from multiple occurrences of the same single concept.

ACSI 33 chapter	**PO**	**AI**	**DS**	**ME**	**Total**
Part 2 - ICT Security Administration					
Chapter 1 - ICT Security Roles and Responsibility	28	1	3		**32**
Chapter 2 - Security Documentation	17	1	3		**21**
Chapter 3 - Identifying and Developing an ICT Security Policy	8			5	**13**
Chapter 4 - Risk Management	20			1	**21**
Chapter 5 - Developing SSP	2		2		**4**
Chapter 6 - Developing and Maintaining Security SOPs	7	9	1		**17**
Chapter 7 - Certifying and Accrediting ICT Systems		12	6	30	**48**
Chapter 8 - Maintaining ICT Security and Managing Security Incidents	8	10	33	5	**56**
Chapter 9 - Reviewing ICT Security				12	**12**
Total Control Objectives in Part 2	**90**	**33**	**48**	**53**	**224**
Part 3 - Security Standards					
Chapter 1 - Physical Security	3		34		**37**
Chapter 2 - Personnel	7		10		**17**
Chapter 3 - ICT Product Life Cycle		18	4		**22**
Chapter 4 - Hardware Security	12		50		**62**
Chapter 5 - Software Security	22	43	41	3	**109**
Chapter 6 - Logical Access Control			44		**44**
Chapter 7 - Active Security	5	9	26	0	**40**
Chapter 8 - Communications Security (Comsec)	5	25	18		**48**
Chapter 9 - Cryptography	6	16	32	1	**55**
Chapter 10 - Network Security	4	6	61	4	**75**
Chapter 11 - Data Transfers	3		19		**22**
Total Control Objectives in Part 3	**67**	**117**	**339**	**8**	**531**
Total Control Objectives in ACSI 33	***157***	***150***	***387***	***61***	***755***

Table 4. Frequency of COBIT's control objectives, presented by COBIT's domains, containing information assurance concepts for each chapter of ACSI 33 (PO: Plan and Organize, AI: Acquire and Implement, DS: Delivery and Support, ME: Monitor and Evaluate).

Figure 1 presents the information assurance-related control objectives from COBIT's IT processes, displayed by alignment to Part 1 and Part 2 of ACSI 33, grouped into the four COBIT domains. This kind of analysis and display provide an overview of where alignment is closest and where it is not. For example, frequent alignment was found between Part 3 of ACIS 33 and specific IT control processes of COBIT, particularly DS5 *Ensure Systems Security*, AI3 *Acquire and Maintain Technology Infrastructure* and DS11, *Manage Data*. These results suggest that where organisations adopt COBIT and achieve a moderate to high level of control over DS5, AI3 and DS11, they are also

likely to comply with at least some of the requirements of ACSI 33's Part 2, *ICT Security Standard*. However, as indicated earlier the frequency of mapping between COBIT and Part 2 of ACSI 33, *ICT Security Administration*, was not as high. Where the alignment is closest to ACSI 33, organisations adopting COBIT may have lower vulnerability to withstand terrorist attack to their ICT systems, while higher vulnerability is expected where alignment to ACSI 33 is lower.

As COBIT's four domains parallel the Systems Development Life Cycle (SDLC), the mapping method followed and the display used also enable analysis from a life cycle perspective. The SDLC is represented in Figure 1 from the bottom of the graph to the top. In the example provided in Figure 1, it can be seen that there is more frequent alignment between the *Acquire and Implement*, and the *Deliver and Support* phases of the life cycle with Part 3 of ACSI 33 on *ICT Security Standard*, while there was more alignment at the *Plan and Organise*, and *Monitor and Evaluate* phases for Part 2 of ACSI 33, on *ICT Security Administration*. From a counter-terrorist perspective, those phases of the life cycle (and IT processes) with smallest alignment between COBIT and ACSI 33 may require first attention to determine the degree of exposure. For example in Figure 1 IT processes to ensure continuous services (DS4) seem to pose more risk than those aimed to ensure systems security (DS5).

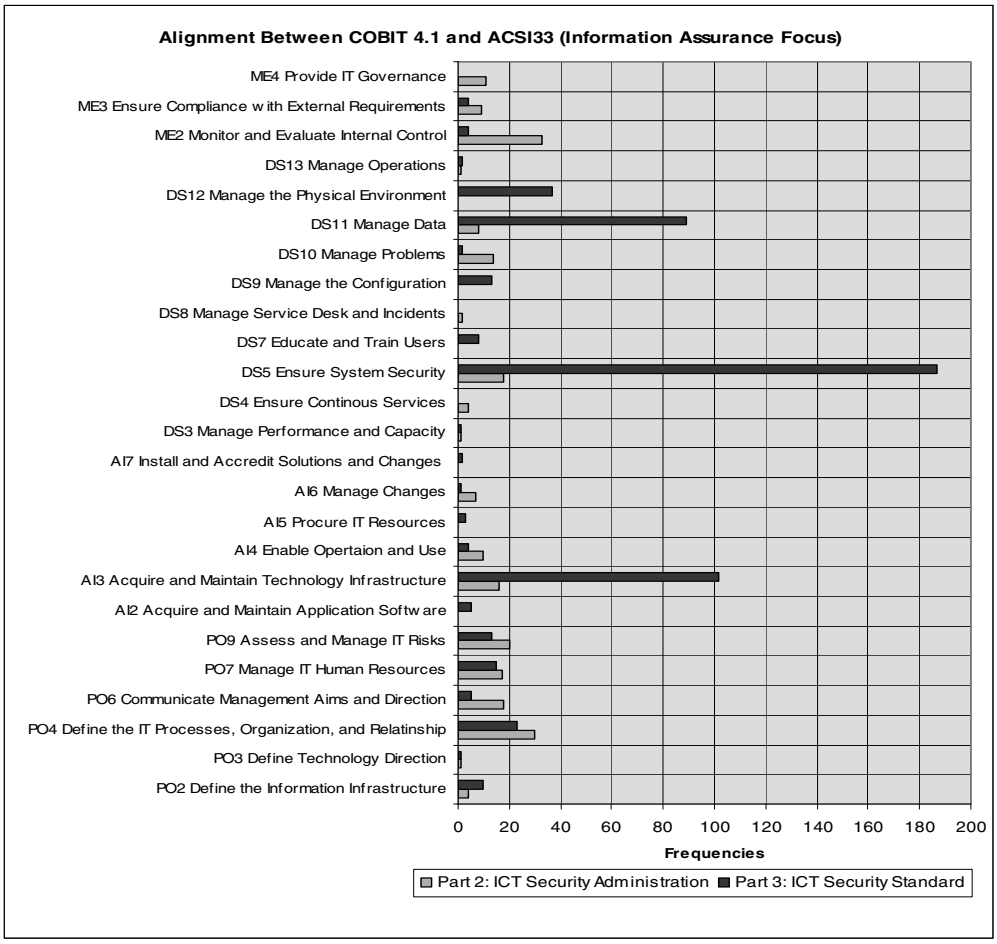

Figure 1. Graph of frequency of information assurance-related control objectives in COBIT's IT processes, mapped to ACSI 33 Part 1 & 2.

The conclusions from the study are considered next.

5 CONCLUSIONS

Practitioner studies have examined the alignment of different IT security standards, and the results have been used in many organisations. However despite this activity, almost no academic-based research has been reported that investigates the alignment of any kind of IT standards. One barrier to this research being undertaken is that it appears that no scholarly method has been identified for analysing the alignment of IT security standards, particularly one that addresses the potential subjectivity of content analysis. The findings of this study suggest that conceptual analysis, a version of content analysis that is novel in an IT security context, is a method that is appropriate for mapping the alignment of IT security-related standards. This study indicates the feasibility of applying Carley's (1993) eight-step process when undertaking content analysis for mapping the alignment of IT security-related standards, even though the standards mapped may be different in nature. Following Carley's (1993) method provides a means of making the process of mapping standards explicit, reducing the risk of subjectivity. The method offers a way of increasing confidence in the results of future studies to map the alignment of IT standards.

By mapping two example IT security-related standards, ACSI 33 and the information assurance elements of COBIT, this study was able to demonstrate the efficacy and the rigour of the method. The method used has potential for the future mapping of other IT security standards. The study provides a method that will enable academics and practitioners to have more confidence in the results of studies into the degree of compliance with one IT security standard when an organisation adopts another to which the first has been mapped.

The results from mapping the two example standards have potential for use to assess compliance with ACSI 33 through voluntary adoption of COBIT, given awareness of the extent and depth of adoption of COBIT. The results of the study also illustrate how knowledge of the alignment of the two specific standards examined offers value within a counter-terrorism context in Australia. The results do so by suggesting some of the vulnerabilities and strengths of private enterprise organisations that adopt COBIT to terrorist attack on their ICT systems, if it is assumed that ACSI 33 provides an appropriate benchmark for this purpose. As much critical infrastructure in many nations is controlled by private sector organisations, the vulnerability of their ICT systems to terrorist attack is worthy of investigation.

For future work the results of mapping IT security standards using the method outlined can also be used for gap analysis. Gap analysis of existing IT security standards offers potential to strengthen future versions of those standards, along with the IT security of organisations that implement them.

Acknowledgements

The Australian Government Department of the Prime Minister and Cabinet has contributed funding to the project, but does not necessarily endorse the contents or conclusions of the work. The valuable comments of the reviewers, associate editor and track chair for ECIS 2008 on an earlier version of this paper are acknowledged with gratitude.

References

Ahlgren, M., Breidne, M. and A. Hektor. (2005). IT security in the USA, Japan and China: A study of initiatives and trends within policy. R&D, industry and technology. Swedish Institute for Growth Policy Studies, Ostersund, Sweden.

AICPA (2007). The AICPA 2007 Top Technology Initiatives. Available: http://infotech.aicpa.org/, Accessed: November 8, 2007.

Allen, J. (2006). Maturity of Practice and Exemplars, Build Security In. Department of Homeland Security. Available: https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/management/567.html, Accessed: 19th June, 2007.

Andrews, D. (1996). Report of the Defense Science Board Task Force on Information Warfare Defense. Office of the Secretary of Defense. Washington DC, USA.

Amoroso D.L. and L.V. Eriksson. (2000). Use of content analysis for studying the creative construct in the context of technology-rich applications. In Proceedings of the 33rd Hawaii International Conference on System Sciences, p. 7041, IEEE Computer Society, Maui, Hawaii.

Brooks, W., Warren, M. and Hutchinson, W. (2002). A security evaluation criteria, Logistics Information Management, 15 (5/6), 377-384.

Brown, W. and Nasuti, F. (2005). What ERP systems can tell us about Sarbanes-Oxley. Information Management & Computer Security, 13 (4), 311-328.

Busch C., Maret S.P., Flynn T., Kellum R., Le S., Meyers B., Saunders M., White R. and M. Palmquist. (2005). Content Analysis. Available at: http://writing .colostate.edu/guides/research/content Accessed: Oct 31, 2007.

Carley K. (1993). Coding choice for textual analysis: A comparison of content analysis and map analysis. Sociological Methodology, 23 (75-126).

Connor, F. and A. Coviello. (2004). Information Security Governance: A call to action. Corporate Governance Task Force Report. Available: www.cyberpartnership.org/InfoSecGov4_04.pdf, Accessed: November 1, 2007.

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. Information Systems Management, 22 (1), 77-85.

DSD (2006). Australian Government Information and Communications Technology Security Manual. September. Commonwealth of Australia, Barton, ACT.

DSD (2007). ACSI 33. Available: http://www.dsd.gov.au/library/infosec/acsi33.html, Accessed November 2.

Hale, J. and Brusil, P. (2004). Secur(e/ity) management: Two sides of the same coin. Journal of Network and Systems Management, 12 (1), 1-8.

Hawkins, K., Alhhajjaj, S. and Kelly, S. (2003). Using COBIT to secure information assets. The Journal of Government Financial Management, 52 (2), 22-32.

Hurley, J. (2005). Best Practices in Security: Governance, Aberdeen Group. Available: http://www.aberdeen.com/summary/report/benchmark/RA_GOVERNANCE_JH.asp, Accessed: November 5, 2007.

ITGI (2000). COBIT Mapping-Mapping of ISO/IEC 17799: 2000 with COBIT. Available: www.isaca.org/cobit, Accessed: November 1, 2007.

ITGI (2007). COBIT 4.1 is now available. Available: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981, Accessed: November 2.

Jauch, R.L, Osborn, N.R. and Martin N.T. (1980). Structure content analysis of case: A complementary method for organizational research. The Academy of Management Review, 5 (4), 517-525.

Romero, P. (2005). An immunological approach to counter-terrorism and infrastructure defense law in electronic domains. International Journal of Law and Information Technology, 14 (1), 101-136.

Texas State Auditor Office (1995). Data analysis: Analyzing data – content analysis. The Texas State Auditor's Offices. Available at: http://www.preciousheart.net/chaplaincy/Auditor_Manual/14conted.pdf, Accessed: Oct 31, 2007.