11-30-2010

An Analytical Study of It Security Governance and its Adoption on Australian Organisations

Tanveer A. Zia
Charles Sturt University

DOI: 10.4225/75/57b52648cd8b1
8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

An Analytical Study of It Security Governance and its Adoption on Australian Organisations

Tanveer A Zia
School of Computing and Mathematics
Charles Sturt University
NSW, Australia
tzia@csu.edu.au

Abstract

Contemporary organisations are at infancy stages of adopting IT governance processes in Australia. Organisations who have adopted these processes underestimate the security processes within the governance framework. If the security processes are designed, they are often flawed with operational level implementation. This study investigates IT security governance broadly and in Australian organisations specifically. The objective of this study is to bring the local organisations in alignment with international standards and frameworks in terms of integration of information security, IT audits, risks and control measures. A survey of selected organisations is completed and results are presented in this paper identifying the maturity level of IT security governance in Australian organisations against the well known Capability Maturity Model® (CMM.)

Keywords

IT security governance, information security, governance standards, risk management, compliance.

INTRODUCTION

This study investigates the national and international standards to show the ways in which values and attitudes are associated with IT (Information Technology) governance aligned with information security in strategic business planning. The complexity of implementing international standards and best practices in information security and IT governance has not been holistically examined within Australian contexts. This paper completes this gap and specifically investigates IT security governance in overall IT governance framework against several national and international standards.

Information security is a global issue. AuSCERT (2006) reported that there were 63% unpatched or unprotected software vulnerabilities which were the cause of experienced harmful electronic attacks. In the same survey, 50% of the respondents who experienced harmful electronic attacks cited that these vulnerabilities were due to insecure misconfigurations on computer networks. "Inadequate staff training and education in security practices and procedures (53%) and inadequate human resources for system hardening and implementing security practices (47%)" were among the most common weaknesses within organisations which lead to network related attacks. Only 10% of the respondents felt that they were managing all computer security issues reasonably well.

This study also contributes towards objectives of The Computer Network Vulnerability Assessment (CNVA) Program which is an Australian Government initiative to support the work of the Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection to identify major vulnerabilities within ICT systems, dependencies between networks, and to test the ability of systems to resist exploitation (CNVA Fact Sheet (2008). Developed by ASIO, TISN is a forum which provides a methodology to identify and prioritise Australia's critical infrastructure and allows users to develop a strategic overview of the risks to their assets. The ultimate objective is to build a more resilient Australia by protecting its information assets.

Despite of its presence in every business process, IT security is often treated solely as a technology issue, when it should be considered as a governance issue. Looking at the increased compliance and governance frameworks it is clear that IT security is not just a technical issue; it has become very much a corporate governance challenge. Due to the wide spread of technology, organisations today face increased scrutiny when it comes to IT security governance Conner, Noonan, and Holleyman (nd). International standards and legislations such as Sarbanes-Oxley Act are creating legal obligations to pay attention to information security and how is it governed.

OVERVIEW

IT organisations have evolved from technology providers into service providers requiring a complete new perspective of IT management (Salle 2004). IT service management puts the services delivered by IT at the centre of IT management and is defined as "a set of processes that cooperate to ensure the quality of IT services" (Young 2004). Security has

become the central focus of IT service management because most of the services are delivered digitally, through wired or mobile ad hoc wireless networks. Service providers are being pushed to enable simplified services that can be well packaged, easy to use and securely delivered, with simplicity and value being the decision points for users and the critical success factors for revenue growth. Silva (2005) has emphasised on removing social, geographical, economic and capacity impediments through provision of cost effective infrastructures**.** Ensuring the management of converged services and networks require radically new approach.

The IT Governance Institute (ITGI 2003) suggests that IT governance is concerned with IT's delivery of value to the business and mitigation of IT risks. IT value delivery is driven by strategic alignment of IT with the business objectives, mitigation of IT risks delivered by embedding accountability into enterprise. This leads five main focus areas of IT governance. Two of them are outcomes: value delivery and risk management. Three are drivers: strategic alignment, resource management, and performance management. In order to deliver security in IT service management and IT governance, strategic alignment of IT and risk management are to be addressed.

Networks have inherent weaknesses and are ever since victim of security threats. Just like information technology, information security is no longer exclusively a technical domain; it has become a management issue. One way to address this is from strategic perspectives; considering it an issue to be addressed in IT governance and organisational policies. Another way to address it is from human perspectives, by embedding information security in organisational culture through awareness, training and the setting of new ethical values. Eloff and Eloff (2003) suggest that information security requires a holistic approach, requiring a combination and integration of information security processes and products. Processes focus on planning and implementing management practices and procedures while products deal with IT infrastructure in order to establish and maintain information security.

In today's harsh economic turmoil, organisations are facing twin challenges of falling profits and skyrocketing costs. There is a stronger need of integration in IT Services and business objectives with information security. A survey of over 1000 CEOs conducted by IBM (IBM Global CEO Study 2008) provides highlights on new and compelling perspectives on strategic issues such as global integration and "change". This change can be addressed by redesigning the way we deliver IT services, performance management of these services, IT governance and addressing the security and privacy issues.

To ensure security in IT governance it is important to integrate security in business processes at all organisational levels and adapt secure system architecture which governs and makes sure that organisational security tasks are deployed correctly. A system architecture (Betz 2006) includes an analysis of the large scale IT capability, with specific attention to business processes, structured data and enabling systems, and suggests adopting a unique value chain approach to integration of COBIT, ITIL, and CMM frameworks into a coherent and detailed conceptual information model mapped to both the processes and systems architecture. However, this architecture overlooks the processes in terms of IT governance and security.

HP (2008) has developed information security service management model to guide organisations to build and run an information security management system within the context of a service management system. This model revolves around six components: compliance of standards and regulations, deployment guidance, applicability of security controls, control implementation specifications. Security management standards such as ISO/IEC 17799, ISO/IEC 27001, and COBIT outline information security controls and their objectives. However, there is a need for detailed design and implementation guidance in these standards. Furthermore, these standards are silent on ad-hoc wireless networks and issues related to performance management. Compliance of these standards in Australian enterprises is rare.

According to CSI Computer Crime and Security Survey (2008) very few organisations have IT security budget allocated more than 10%. 53% of the organisations allocated 5% or less of their IT budget to information security (See Figure 1).

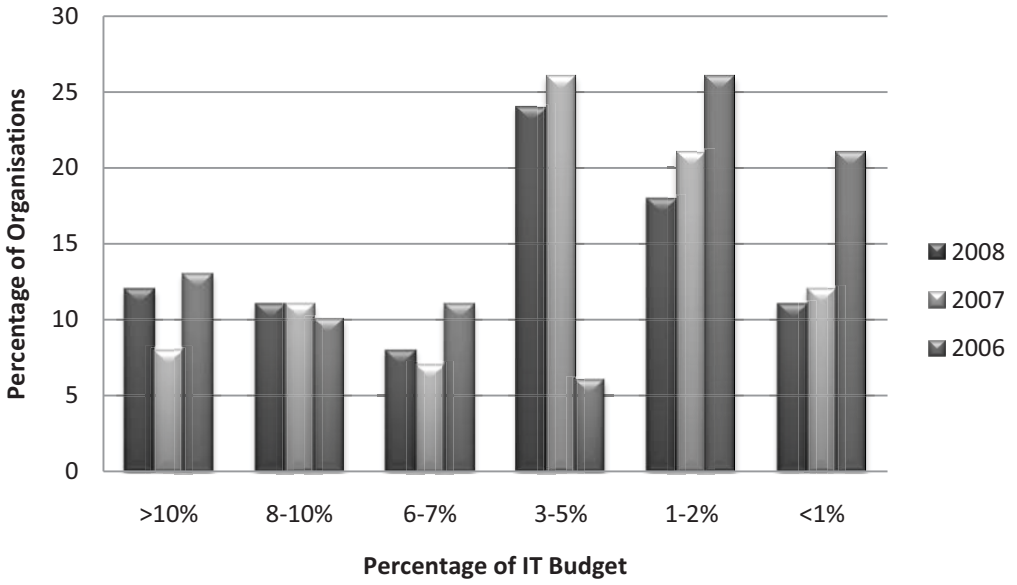

Figure 1: IT Security budget allocation

This is in contrast interesting that awareness about IT security is much higher with 67% organisations having formal information security policy established (Figure 2).

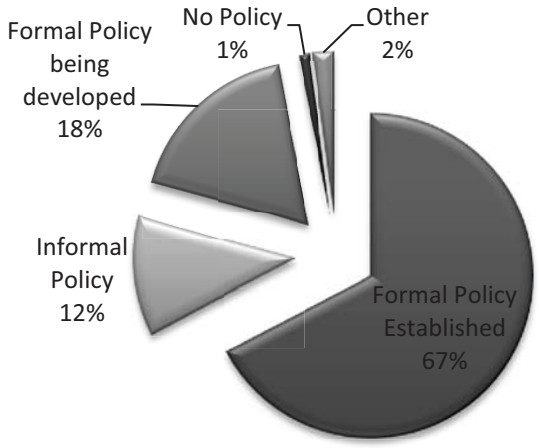

Figure 2: Information security policy

In another survey conducted by AusCERT (Australian Computer Emergency Response Team), 2006, vendor and industry specific IT security policies were on increase in 2006 (See Figure 3). This survey shows decline in adoption of national and international IT security standards.

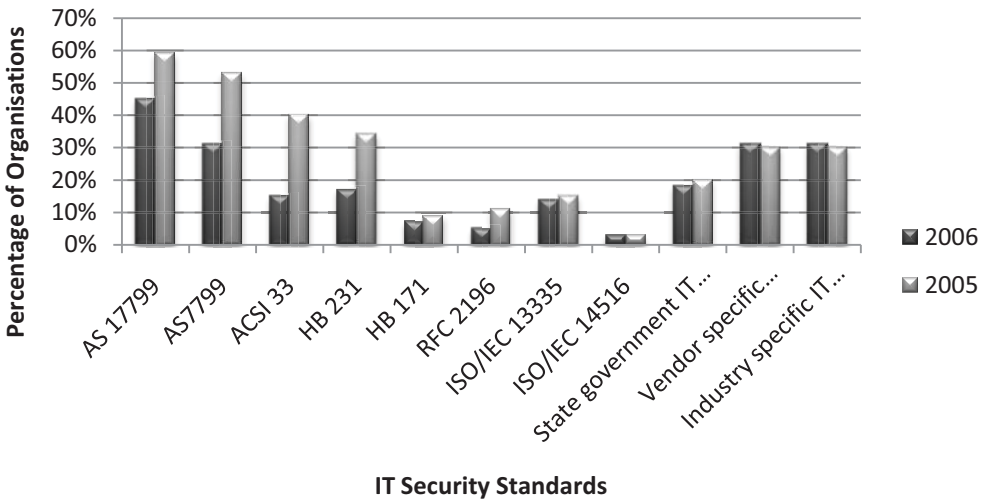

Figure 3: IT security related standards used in Australia (Australian Computer Crime and Security Survey 2006)

IT GOVERNANCE FRAMEWORKS AND STANDARDS

IT Governance is fundamentally about answering two questions: how IT delivers value to the business and how IT risks are mitigated. There are several IT governance frameworks and standards. For the purpose of this study we review CobiT, COSO, and ISO/IEC 27000.

Control Objectives for Information and Related Technologies (CobiT) is created by the IT Governance Institute (ITGI) which is part of the Information Systems Audit and Control Association (ISACA). ISACA is the professional body of IT auditing Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM) certifications. There are 34 IT processes organised in four inter related domains in CobiT framework. Table 1 describes the four CobiT domains and number of processes in each domain. CobiT focuses specifically on controlling the entire IT function.

Table 1: CobiT domains

CobiT domains	Description
Planning and organisation (PO) (10 processes)	This domain covers strategy and tactics concerning the identification of ways IT can best contribute towards achievement of the business objectives.
Acquisition and implementation (AI) (7 processes)	This domain concerns the acquisition and implementation of IT strategies and IT solutions.
Delivery and support (DS) (13 processes)	This domain is concern with actual delivery of required services
Monitoring and Evaluation (ME) (4 processes)	This domain addresses performance management, monitoring and control, regulator compliance and governance.

Committee of Sponsoring Organisations of the Treadway Commission (COSO) has produced a document called Internal Control – Internal Framework. The Sarbanes-Oxley Act of 2002 specifically requires organisations to use a well-developed comprehensive framework for financial controls and compliance. Therefore, COSO focuses more broadly on corporate internal and financial controls. In COSO framework there are three objectives and five components as shown in Table 2 and 3:

Table 2: three COSO objectives

Objectives	Description
Operations	in order for an organisation to operate effectively it must control its internal operations
Financial reporting	the firm must create accurate financial reports
Compliance	Effectively required for Sarbanes-Oxley compliance

Table 3: five COSO components

COSO components	Description
Control environment	This components is the organisations control environment set by top management. If the control environment is weak other control elements are not likely to be effective
Risk Assessment	An ongoing preoccupation of systematic risk analysis
Control activities	A general policy and set of specific procedures to implement and maintain the controls
Monitoring	Human vigilance and audit trails in IT
Information and communication	Ensures that there is information and communication across all levels in the organisation

ISO/IEC 27000 or ISO 27K is a series of standards for information security developed and being developed by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). The first standard in the series was called ISO/IEC 17799. When it was decided to have all security standards begin with 27000, this standard was renamed to ISO/IEC 27002. In 2005, ISO/IEC 27001 was released to specify how to certify organisations as being compliant with ISO/IEC 27002. ISO/IEC 27002 divides security into 11 broad areas:

- Security policy
- Organisation of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information security incident management
- Business continuity management
- Compliance

These areas are subdivided into many more specific elements. ISO/IEC is working on a number of other standards for the 27000 series. A summary of standards developed or being developed (ISO27001 Security, 2010) is provided in Appendix A.

The Australian implementation for ISO/IEC 27001:2005 is AS/NZS ISO/IEC 27001:2006. Some other standards and guidelines which have been made obsolete or superseded by new standards are:

HB 171:2003	A handbook for the management of IT evidence published by Standards Australia
HB 231:2004	Information security risk management guidelines published by Standards Australia
RFC 2196	Site security handbook published by Internet Engineering Task Force (IETF)
ISO/IEC 13335-1:2004	Management of ICT security
ISO/IEC 14516:2002	IT security techniques: guidelines for the use and management of Trusted Third party services.

Several organisations around the globe have adopted IT Governance and have complied with CobiT framework (CobiT Case Studies, 2010). Table 4 provides examples of some organisations:

Table 4: Organisations and their rationale for CobiT adoption

Organisation	*Rationale for adopting CobiT*
Sun Microsystems, USA	Supports IT control and audit activities in light of Sarbanes-Oxley Act.
Adnoc Distributions, UAE	Offers a complete framework to address all the elements of a process and key performance indicators. CobiT is used in conjunction with ISO27001, PMBOK and portions of ITIL.
Central Bank of the Republic of Armenia	IT audit and risk assessments because of its internationally recognised reputation
Kuwait Turk Participation Bank	Easily maps with other leading standards
Canadian Tire Financial Services, Ltd	Bridges It and business processes and provides effective control for IT related processes
Prudential, Asia	Achieves enhanced communication between IT and business processes
Government of Dubai	Provides control objectives and improves IT governance
Bahrain Civil Service Bureau	A most comprehensive and globally respected framework for implementing IT governance
Coopers & Lybrand, Netherlands	Improves client IT department procedures
Security Audit and Control Solutions, South Africa	Provides a comprehensive control and risk assessment

Although some Australian organisations have also deployed the CobiT framework as shown in Table 5, there are other IT governance frameworks, standards and regulations equally deployed in Australian corporations.

Table 5: Deployment of CobiT in Australian organisations

Organisation	*Rationale for adopting CobiT*
Curtin University of Technology	Audits as an opportunity to plan improvements
Australian Governmental Organisation, Canberra	A comprehensive framework for deployment of control, audit and testing strategies
New South Wales Health	Identifies risks and offers effective controls to mitigate risks

DATA COLLECTION AND ANALYSIS

A survey questionnaire (Appendix A) was compiled and used to collect data from selected Australian organisations those have adopted IT security and audit controls. This data is analysed in context of CobiT, COSO and ISO/IEC 27K for the best practices in information security governance. CMM is used to determine the maturity of IT Security Governance in Australian organisations. The rationale for using these standards and verification through CMM is to establish the notion of maturity, how well Australian organisations are doing in adopting national and international standards and where they stand in terms of compliance.

Initially 20 organisations were contacted to complete the survey. Ten organisations responded to the survey. We have categorised the surveyed organisations into two categories: Government (four organisations) and non-government (six organisations). Some of the survey results are summarised in Table 6.

To determine the maturity of the organisations capability to deploy its Information Security and Risk Management Strategy (ISRM) successfully we have used CMM (Capability Maturity Model) (Paulk et. Al 1995). CMM is a tool developed by the Software Engineering Institute (SEI) at Carnegie Mellon University. Organisations surveyed are assessed against the five maturity levels of the CMM (See Table 7).

Table 6: Survey on IT security governance

Survey Parameters	*Government Organisations*	*Non-Government Organisations*
Presence of Information Security Management System	Yes	Yes
Highest level IT security role	Security Manager	Chief Information Security Officer (CISO)
Responsible for IT Risks	CIO	CEO
Percent of budget allocation in IT Security/Risk Management	Less than 1%	8-10%
Standards adopted	ITIL, AS/NZS ISO/IEC 27001:2006, Risk IT	ITIL, PMBOK, ISO/IEC 17799:2005, AS/NZS ISO/IEC 27001:2006, Risk IT
Threats to IT Assets	Viruses, Unauthorised access, system penetration, website defacement, abuse/misuse of IT resources	DoS, Viruses, laptop theft, insider abuse, password sniffing, theft of customer data, unauthorised access, system penetration, website defacement, theft/loss of proprietary information, abuse of wireless networks, abuse/misuse of IT resources.

Table 7: Capability Maturity Model

Maturity Level	General description	Control summary
0	Non-existent, intent and not identified	Controls not present Not implemented
1	Initial, undefined and ad-hoc	Not officially assigned to an individual Not documented Not monitored
2	Repeatable, reactive and intuitive	Ownership is assigned Documented via policies and guidelines Inconsistent implementation
3	Proactive, defined and implemented	Owners are trained to operate Documented standards Evenly implemented
4	Managed, controlled and measureable	Controls are audited and tested Standards in place and followed Operate within recognised processes
5	Optimal, optimizing and business-aligned	Controls are included in regular audit and assessment Monitored and measured Complete control quality assurance

Analysing the survey results we place IT Security and Risks management in government organisations at CMM Maturity Level 1. This means IT risks management is ad-hoc and at initial stages. IT risks are dependent on individual projects and there is informal risk management. Senior management has little interests in managing day to day IT risks. This is further verified by the fact that the highest level of IT security position is IT security Manager. This is indicator that IT security management is not addressed at highest organisational level.

Maturity level of IT security governance in non-government organisations is much higher and resides between CMM Maturity level 3 and 4. This means that security processes are well documented and organisations have well defined IT security policy and risk management strategies. Senior management is well informed about the security risks and takes the security very seriously. Presence of Chief Information Security Officer (CISO) in board level is an indicator that IT security governance is one of the top priorities. Addressing the IT security and management of risks in non-government organisations seems to be in aligned with international organisations.

CONCLUSION AND FUTURE WORK

This paper has addressed an important aspect of corporate governance: IT security governance. Several standards and their implementation are reviewed. A survey of IT security governance in Australian organisations is conducted categorising the organisations into government and non-government. According to the survey results, it is determined that IT security governance in non-government organisation is more mature as compare to the government organisations.

In future, the survey will be extended to include more organisations in conjunction with face to face interviews wherever possible. An electronic survey would be developed and at least ten more organisations would be invited to complete the survey, out of which informants from five organisations will be chosen for semi-structured interviews. The selection of organisations will depend on the degree of alignment of their IT processes with IT governance frameworks and standards. Case studies of international organisations with established record and best practices in IT security governance will be analysed and compared with the Australian context. This will involve evaluating organisations both Australian and international against the IT governance frameworks and standards set by COBIT, ITIL, CMM and in security ISO/IEC 27002:2005, ISO/IEC 17799:2006, and COSO.

NOTE

(1) This work is supported by Charles Sturt University Small Grant projects and some preliminary results from the study are presented at the Information Technology Security Conference (ITS 2010).

REFERENCES

AusCERT (2006) “Computer Crime & Security Survey.” Retrieved July 10, 2010 http://www.auscert.org.au/images/ACCSS2006.pdf

Betz, C. (2006) "Architecture and patterns for IT service management, resource planning, and governance: making shoes for the cobbler's children." MO, USA. Elsevier.

CNVA Fact Sheet (2008) "TISN (Trusted Information Sharing Network)." Retrieved June 28, 2009 from http://www.tisn.gov.au/

CobiT (2008) "Control Objectives for Information and related Technology." Retrieved December 30, 2008 from http://www.isaca.org

CobiT (2010) "Case studies" Retrieved July 12, 2010 from https://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Studies.aspx

Conner, B., Noonan, T. and Holleyman, R. W. (nd). "Information Security Governance: Toward a Framework for Action." Retrieved July 12, 2010 from http://www.bsa.org

Computer Security Institute (CSI) (2008) "Computer Crime and Security Survey." Retrieved July 10, 2010 from http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf

Eloff, J. H. P. and Eloff, M. (2003) "Information security management: a new paradigm." Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology.

Forbes. (2009) "The Global 2000: Special report." Retrieved October 7, 2009 from http://www.forbes.com/lists/2009/18/global-09_The-Global-2000-Australia_10Rank.html

HP. (2008) "Information Security and Service Management for State & Local Governments." Retrieved January 9, 2010 from http://media.govtech.net/HP_RC_08/Security_RC/ISSM_for_SLG.pdf

IBM (2008) "Global CEO Study." Retrieved July 10, 2010 from http://www-935.ibm.com/services/us/gbs/bus/pdf/ceo-study-executive-summary.pdf

IBM (2004) "IBM and the IT Infrastructure Library." Retrieved July 10, 2010 from http://www-935.ibm.com/services/us/igs/pdf/wp-g510-3008-03f-supports-provides-itil-capabilities-solutions.pdf

ISO27001 Security (2010) Retrieved July 10, 2010 http://www.iso27001security.com/index.html

ITGI (2003) "Board briefing on IT Governance." Retrieved July 10, 2010 from http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=39649

Microsoft (2008) "Microsoft Operations Framework 4.0" Retrieved July 12, 2010 from http://technet.microsoft.com/en-us/library/cc506049.aspx

Panko, R. J. (2010) "Corporate Computer and Network Security (2/ed)." Upper Saddle River, NJ. Prentice Hall.

Paulk, M.C., Weber, C.V., Curtis, B, Chrissis, M. B. (1995) "The Capability Maturity Model: Guidelines for improving the Software Process." Boston. Addison Wesley

Salle, M. (2004) "IT Service Management and IT Governance: Review, comparative analysis and their impact on utility computing." Palo Alto, HP Labs.

Silva, J. S. (2005) "Challenges and opportunities in ICT: A European perspective." Proceedings of the 6th International conference on Mobile data management (MDm'05). NY, ACM Press.

Slay, J. and Koronios, A. (2006) "Information Technology Security and Risk Management." Milton QLD. John Wiley & Sons Australia Ltd

Young, C. M. (2004) "An introduction to IT service management." Research Notes, COM-10-8287, Gartner.

Appendix A – Summary of ISO/IEC standards

ISO/SEC27K series	Description
ISO/IEC 27001:2005	is the information security management system (ISMS) requirements standard
ISO/IEC 27002:2005	is the code of practice for information security management describing a comprehensive set of information security control objectives
ISO/IEC 27003	provides implementation guidance for ISO/IEC 27001
ISO/IEC 27004	is an information security management measurement standards suggesting metrics to help improve the effectiveness of ISMS
ISO/IEC 27005:2008	is an information security risk management standard
ISO/IEC 27006:2007	is a guide to the certification or registration process for accredited ISMS certification or registration bodies
ISO/IEC 27007	will be a guideline for auditing information security management systems
ISO/IEC 27008	will provide guidance on auditing information security controls
ISO/IEC 27010	will provide guidance on information security management for sector-to-sector communications
ISO/IEC 27011:2008	is the information security management guideline for telecommunications organisations
ISO/IEC 27013	will provide guidance on the integrated implementation of ISO/IEC 20000-1
ISO/IEC 27014	will cover information security governance
ISO/IEC 27015	will provide information security management systems guidance for financial service organisations
ISO/IEC 27031	will be an ICT-focused standard on business continuity
ISO/IEC 27032	will provide guidelines for cyber security
ISO/IEC 27033	will replace the multi-part ISO/IEC 18028 standard on IT network security
ISO/IEC 27034	will provide guidelines for application security
ISO/IEC 27035	will replace ISO TR 18044 on security incident management
ISO/IEC 27036	guideline for security of outsourcing
ISO/IEC 27037	guideline for digital evidence
ISO 27799:2008	provides health sector specific ISMS implementation guidance based on ISO/IEC 27002

Appendix B – IT Risk and Security Governance Survey

This survey is part of a study being conducted at Charles Sturt University to determine maturity level of IT Security Governance in Australian organisations. All responses and data collected are highly confidential. At no stage this data will be used other than the above mentioned purpose. *(Please tick the boxes and/or write your response wherever applicable)*

1. Does your organisation have ISMS (Information Security Management System)?
   ☐Yes ☐ No

2. What is the highest level of IT security position in your organisation?

   ☐ CISO
   ☐ Security Manager
   ☐ Security Admin
   ☐ Security Technician
   ☐ Other _____

3. Who has the responsibility and accountability for IT Risks:
   ☐ CEO
   ☐ CFO
   ☐ CIO
   ☐ CISO
   ☐ CISSO
   ☐ Other _____

4. Does the organisation maintain an IT risk register?
   ☐Yes ☐ No

5. How often is the risk register updated?

☐Quarterly ☐ Yearly ☐ Other _____

6. How are IT risks communicated to all stakeholders in organisations?
   ☐ Induction/Training
   ☐ Professional Development

7. How are the risks classified in your organisation?
   ☐ avoidance
   ☐ mitigation
   ☐ transfer
   ☐ acceptance

8. How does the organisation manage IT Risks?

   ☐ Risk assessment for processes and business decisions does not occur
   ☐ Risk management is not identified as relevant to acquiring IT solutions and delivering IT services
   ☐ IT Risks are considered in an ad hoc manner
   ☐ Informal assessments of project risk take place as determined by each project
   ☐ Risk assessment approach exists and is implemented at the discretion of the project managers
   ☐ The risk management is usually at a high level and is typically applied to only major projects
   ☐ An organisation wide risk management policy is available.
   ☐ Risk management is defined process that is documented
   ☐ The assessment and management of risk are standard procedures
   ☐ Risk is assessed and mitigated at the individual project level
   ☐ Risk management is structured, organisation wide process and is enforced
   ☐ Risk management is truly integrated in all IT operations

9. Percent of organisation budget spent in IT?
   ☐ more than 10% ☐ 8-10%
   ☐ 6-7% ☐ 3-5 %
   ☐ 1-2 % ☐ less than 1%

10. Percent of organisation budget spent in IT Security/Risk Management?
    ☐ more than 10% ☐ 8-10%
    ☐ 6-7% ☐ 3-5 %
    ☐ 1-2 % ☐ less than 1%

11. Frequency of review of the IT risk management process.
    ☐Quarterly ☐ Yearly ☐ Other _____

12. Percent of identified IT events used in risk assessment? _____ %

13. Percent of identified critical IT events that have been assessed? _____ %

14. Percent of risk management action plans approved for implementation. _____ %

15. Percent/Number of significant incidents caused by risks that were not identified by the risk assessment process? _____ %

16. What is the governance structure for information security in the organisation? Please draw if different than below.

    CEO
    ⇧
    CIO
    ⇧
    CISO
    ⇧
    Security Manager
    ⇧

Security Admin
⇧
Security Technician Other *(please draw the structure)*

17. What standard(s) and/or framework(s) does your organisation complies with?
☐ ITIL (for service delivery)
☐ CMM (for solution delivery)
☐ PMBOK or PRINCE2 (for Project Management
☐ ISO/IEC 17799:2005 (for information security)
☐ AS/NZS ISO/IEC 27001:2006 (for information security)
☐ COBIT (for IT Governance)
☐ Val IT (for IT Governance)
☐ Risk IT (for IT Risk Management)
☐ Other _____

18. What are the organisation's business objectives?
☐ Revenue and Market Share
☐ Reputation and Brand
☐ Asset and Capital Management
☐ Earnings and Operating margins
☐ Others _____

19. What are possible risks the organisation faces?
☐ Economic conditions
☐ Price volatility
☐ Interest rate volatility
☐ New product development
☐ Environmental regulation
☐ Government regulation
☐ IT infrastructure capacity
☐ Key supplier dependence
☐ Recruitment and retention
☐ Customer migration
☐ Regulator compliance
☐ Others_____

20. What are the organisational business processes?
☐ Product development
☐ Sales and marketing
☐ Customer support
☐ Production
☐ Procurement
☐ Others _____

21. What are organisational IT Assets?
☐ IT Infrastructure
☐ Network
☐ Applications
☐ Databases
☐ Others _____

22. What are threats to your organisational IT Assets?

☐ Denial of service	☐ laptop theft	☐ Telecom fraud	☐ Unauthorised access
☐ Viruses	☐ Insider abuse	☐ Financial fraud	☐ System penetration
☐Sabotage	☐ Bots	☐ Password sniffing	☐ Website defacement
☐ Theft/loss of proprietary information		☐Theft/loss of customer data	
☐ Abuse of wireless network		☐ Misuse of web application	

☐ Abuse/misuse of IT resources ☐ Others _____

Would you be interested and available for a face to face interview for a similar study?
If Yes, what is your availability ☐ 1-2 week notice ☐ 3-4 week notice ☐ Other _____

Please provide contact details:
Name: _____ Position: _____
Organisation: _____
Email: _____Phone: _____

Thank you for completing the survey. Please send the completed survey to xxx.