Trusted Information Sharing Network

for Critical Infrastructure Protection

CIO, CISO and Practitioner Guidance

IT Security Governance

June 2006

(Revision 1, August 2007)

(Revision 2, December 2009)

SEC: PUBLIC

CIO, CISO and Practitioner Guidance

Whatever your business, security and privacy are key matters that affect your enterprise and those dependent upon you. There is a realisation, domestically and abroad, that an organisation cannot effectively achieve its corporate and IT governance objectives without high-level executive support. These issues are now reaching boardroom agendas via an increasing awareness that a strong and effective IT security governance framework is fundamental to achieving organisational objectives, meeting stakeholder requirements, maintaining compliance with laws and regulations and maintaining acceptable levels of risk across the enterprise.

It is important to understand your role in planning, implementing and maintaining IT security governance within your organisation. You have an obligation to promote IT security governance throughout the enterprise.

This paper works as a reference guideline for CIOs, CISOs and their respective security management practitioners, highlighting the importance of an appropriate governance framework for the management of corporate information networks and IT security to ensure the continuity of critical infrastructure services. It covers what you need to know and what is expected of you.

What is IT security governance?

While there are many characteristics to IT security governance, an all-inclusive definition is difficult to contextualise. Leading practice dictates that IT security governance defines the core IT security principles, the accountabilities and actions of an organisation, to ensure that its objectives are achieved.

Through research and consultation, a list of essential attributes of IT security governance was developed and consequently led to the definition to the right.

IT Security Governance

"Establish and uphold a culture of IT security to provide assurance that the business objectives and stakeholder requirements for the protection of information are continually met."

It is important to demonstrate how IT security governance aligns with the other governing areas that affect organisations. The figure below highlights how corporate governance serves as the overall framework for driving all governance activities within the organisation.
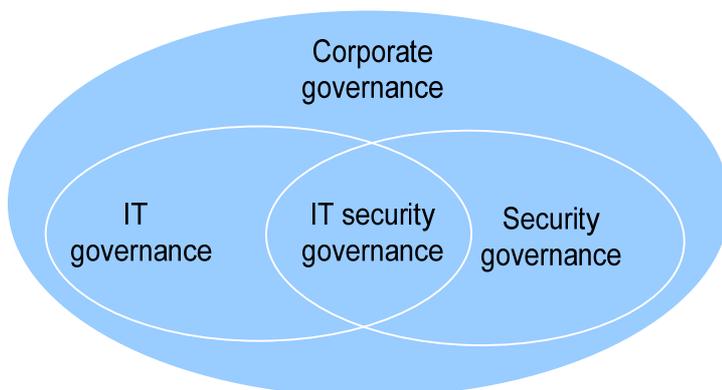
IT governance provides outcomes specifically focused on aligning IT with the business while security governance provides outcomes specifically focused on aligning security with the business, including both physical and IT security.

Figure 1- Corporate, IT and security governance relationships

As depicted, IT governance and security governance contain a number of similar attributes which is IT security governance. The different focus of IT governance and security governance results in an overlap of activities, with this distinction ensureing that the IT security governance framework is not solely driven from an IT point of view.

IT security governance sets the tone at the top for implementing a culture of accountability in order for effective IT security management to take place. In simple terms, IT security governance is used to ensure that all IT security management functions are designed, implemented and operating effectively.

As with all governance mechanisms, IT security governance should be driven by the level of risk to the organisation.

Why is IT Security Governance important?

A strong increase in technology adoption, technology convergence and the growing use of standard technologies has made it essential that all critical infrastructure industries focus on securing their information and assets.

The intangible impacts to trust, reputation and economic and social confidence are often said to be an order of magnitude larger than the tangible impacts and may never be truly understood. In fact, the capability to measure the downstream impacts of an incident (impacts external to the organisation directly affected) are not in place.

What has changed since 2007?

2009 has seen a shift in IT security governance drivers and threats affecting organisations:

- Recent economic conditions have focussed IT security governance activities on addressing audit and compliance requirements while demonstrating the value that security can provide to the business.

- New technologies and sourcing solutions continue to be embraced by organisations at an increasing rate. The increase in demand for more mobile, collaborative and consolidated environments along with the expansion of cloud computing and other hosted services have introduced new IT security governance considerations that need to be balanced with business need.

- The "consumerisation" of IT is leading to individuals adopted new technology before businesses. As an example, Blackberry phones were initially adopted by business, whereas the iPhone has been adopted by individuals, with individuals then expecting that the technology will be integrated into existing business systems. E.g. access to business email through a private iPhone.

- In addition to the "consumerisation" of IT, individuals and businesses are allowing greater freedom around access to environments, including individuals accessing their employers internal network using a private laptop. This trend increases the "deperimeterisation" of business networks which began with the introduction of VPNs and remote access.

2009 Trends and observations

- Increased focus on compliance and value of security.
- Faster adoption of new technology
- "Consumerisation" of IT, with new technology being adopted by consumers before businesses
- Expanding use of virtualisation and consolidation
- Demand for social computing and collaborative environments
- Demand for more mobile environments
- Decreasing cost of high volume portable storage
- Increased use of sourcing models, hosted services and cloud computing
- Increase in social engineering attacks
- Increasingly malicious malware variants
- Increasing threat of nation-state attacks

- Social networking and the related risks associated with data leakage (of sensitive information about the organisation and the people that work in it) has emerged as a growing concern that security professionals must monitor.

- A number of new and old threats are also affecting Australian organisations and critical infrastructure providers. Social engineering (specifically phishing and identity theft), malware

infections (such as Conficker) and reports of nation-state based computer attacks are some of the threats that have increased since 2007.

Owners and operators of critical infrastructure require strong IT security governance to ensure effective ongoing management of these and other threats. The chapters below provides more detail regarding some of these threats.

What threats and risks do I need to consider?

With the risks and threats to IT security dynamically changing, organisations require strong IT security governance to ensure effective ongoing management of risk. The Australian Government Cyber Security Strategy[1] states that "…cyber security is now one of Australia's top tier national security priorities.…..As the quantity and value of electronic information has increased so too have the efforts of criminals and other malicious actors who have embraced the Internet as a more anonymous, convenient and profitable way of carrying out their activities".

The following list, which is not intended to be considered all-inclusive, represents categories that have been identified as key risks that organisations must consider in regards to IT security governance:

Adoption of new technology and hosted services – dependencies on technology, the rate of convergence, the increasing gap between technology adoption and the controls adoption has created a riskier environment where the opportunities for threats are greater than ever before. Examples such as the rapid and widespread adoption of mobile devices and the increase in use of hosted services (including 'cloud' offerings such as Google Docs) can lead to situations where organisations face a gap between the rate of technology adoption and the rate of controls adoption to address any risks. This threat is highlighted with the rapid adoption of iPhones by individuals, with the expectation they will be allowed to access their business email. This expectation has placed pressure on IT security management to relax existing policies and threat and risk assessment mechanisms. It should also be noted that providers of hosted services may not be aware of all possible vulnerabilities and may not have appropriate prevention, detection or response mechanisms to address any issues. Leading practices demonstrate that IT security governance and management activities should be driven from a risk management point of view.

Figure 2 - IT adoption vs. controls adoption
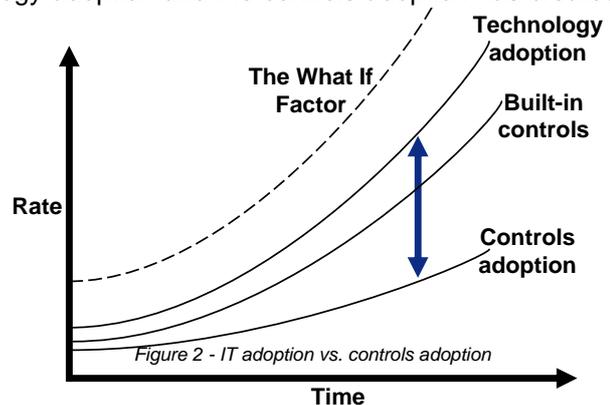
Malicious software – viruses, worms and spyware, are becoming ever more complex and disruptive. Malicious software (or Malware) is increasingly being linked to organised criminal activity whether it be for financial gain, political tactics or general pandemonium. Legacy systems, historically treated as self-sufficient systems, can no longer be ignored; they are just as susceptible to attack as any other network based system.

Human error – can be considered inevitable but the number of incidents related to human error can be prevented and reduced considerably with effective governance. Increasing user awareness to security issues is also essential to combat the increases in social engineering threats such as phishing. This category also includes people's failure to act, and their lack of accountability.

---

[1] Commonwealth of Australia, "Cyber Security Strategy", 2009

Did you know?

In October 2009, thousands of users from three of the largest web-based email service providers (Hotmail, Google and Yahoo!) fell victim to a large-scale phishing attack which tricked users into revealing their credentials. *(Source: The Australian 07 October 2009)*

System failure – system, infrastructure and application failures can have a high impact, especially in critical infrastructure industries where ageing legacy systems are predominately found. Lack of security measures in place for early detection generally contributes to the extent of the impact.

Cyber crime and nation state attacks – **Error! Reference source not found.**The *Australian Business Assessment of Computer User Security: a national survey* released by the Australian Institute of Crimonology in 2009 identified that the total financial loss as a result of computer security incidents against businesses in Australia during the 2006-2007 financial year was estimated at between $595m and $649m.

Identity security – with the increasing interaction between organisations and individuals occurring electronically, the ability to establish trust and confidence in the relationship is critical. Given Australia's identity management systems have traditionally relied upon government issued, paper-based documents and cards, these mechanisms are under pressure. The demand for online interactions with organisations, including critical infrastructure providers, will continue to grow as technology develops and the type, value and complexity of business activities conducted online continue to expand. IT security governance mechanisms will need to adapt to incorporate the increased need to verify an individual's identity to respond to the increasing demand of trust and confidence.

Given the changes to the risk landscape and the continually changing threat environment, this trend is expected to continue. Without a strong focus being placed on enterprise security governance in both public and private organisations, Australian organisations are at risk.

What do I need to do?

Critical infrastructure providers need to satisfy a number of important stakeholders which may include government organisations, regulators, board executives, shareholders and the Australian public. These stakeholders need to trust in an organisation's diligent protection of its information, including privacy and identity, and assets. Once all stakeholders have been identified, CIOs/CISOs should ensure that they understand what is expected and required in regards to IT security governance.

In keeping with the holistic accountability theme of IT security governance, stakeholders generally expect the following from the CIO/CISO:

1. Provide guidelines for accepted IT security practice;

2. Ensure that security practices are integrated into the organisation's strategic and operational planning processes;

3. Ensure business units develop and maintain security programs;

4. Ensure reporting occurs;

5. Ensure awareness programs are in effect to educate individuals in security matters. Evidence that there is awareness i.e. code of conduct IT/Security relevance;

6. Ensure that mechanisms are in place to monitor the changing security threat landscape over time and adjust control environments accordingly;

7. Ensure the implementation, monitoring and review of security (security strategy) including alignment to legislative and best practice standards; and

8   Ensure internal and external audits occur, with adequate plans in place to remediate findings.

Do I need executive buy-in?

IT security governance should be seen as a business success objective. It is all about what level of risk an organisation and its stakeholders are willing to accept. Every executive needs to understand that it should be addressed with the same logic that is applied to make financial, acquisition and other 'non-security' related business decisions.

What is a good framework?

There is no single leading practice model defined for security governance. Each organisation's security risk profile will differ and each organisation's business objectives and practices will differ (even within the same industry). Therefore, it is important to recognise that any model must be adapted and tailored to the individual organisational needs.

Based upon the research and consultations, the following figure represents a leading practice framework which illustrates the key components for security governance via a top-down approach.
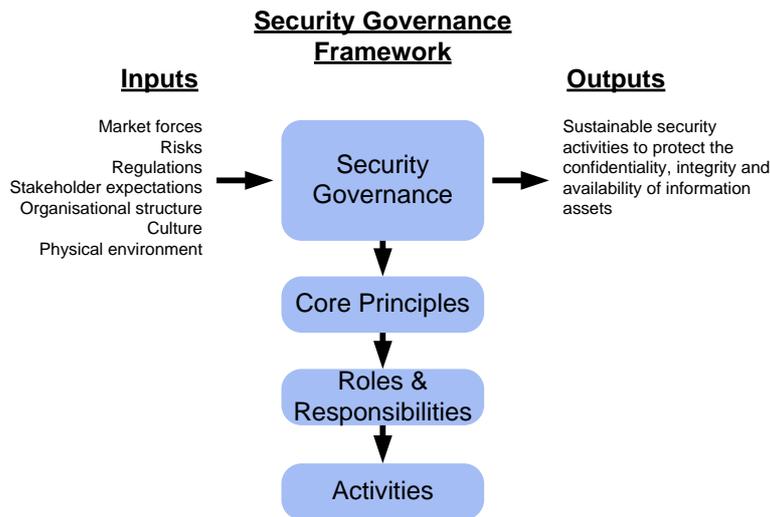
Security Governance Framework

Inputs		Outputs
Market forces Risks Regulations Stakeholder expectations Organisational structure Culture Physical environment	→ Security Governance →	Sustainable security activities to protect the confidentiality, integrity and availability of information assets
	↓	
	Core Principles	
	↓	
	Roles & Responsibilities	
	↓	
	Activities	

Figure 3 - Leading practice security governance framework

This framework is composed of three components:

1 **Core principles** – serve as the primary driver for all IT security governance functions and activities. The eleven principles listed below are not intended to be prescriptive and are provided as a reference guide to build enhanced capabilities, manage security risk, provide an appropriate level of transparency, optimise performance and maximise accountability.

Core principles	
Accountability	Transparency
Awareness	Measurement and Reporting
Compliance	Scope
Effectiveness	Response
Ethics	Risk Management
Inclusion	

2 **Roles & responsibilities** – define the assignment of accountabilities to ensure IT security governance activities take place and achieve the spirit of the core principles. IT security governance framework models should take a view of people, process and technology factors to achieve the following objectives:

- Propose an oversight and management function hierarchy;

- Establish IT security governance as a core function alongside other key corporate governance functions, such as financial and operational risk management; and

- Provide a reference guide for those implementing IT security governance within a corporate governance environment.

3 **Activities** – the underlying processes that are owned and operated by accountable individuals to implement and maintain IT security governance capabilities. It can also be stated that security, as an activity itself must be integrated into an organisation's core functions and processes. The recommended activities for owners and operators of critical infrastructure are as follows:

- Conduct an annual security evaluation, review the evaluation results with staff, and report on performance to the board of directors;

- Conduct periodic risk assessments of information and IT assets as part of a risk management program;

- Conduct threat and risk assessments (TRAs) for any new IT systems or major changes to existing systems. In addition, TRAs should be periodically updated, in a period commensurate with the risk to the system;

- Implement and maintain policies and procedures based on risk assessments to secure its information and assets based on industry sound practice. The core domains in ISO 27002 (formerly ISO17799) describes one such standard which can be used to do this.

- Establish a security management structure to assign explicit individual roles, responsibilities, authority, and accountability;

- Develop plans and initiate actions to provide adequate security for networks, facilities, systems and information;

- Treat security as an integral part of the system lifecycle;

- Provide security awareness training and education to all personnel;

- Conduct periodic testing and evaluation of the effectiveness of security policies and procedures;

- Create and execute remediation action plans to address any security deficiencies;

- Develop, implement and regularly test incident response procedures;

- Establish plans, procedures and tests to provide continuity of operations; and

- Use security best practices guidance to measure security performance, such as ISO17799/ISO27001.

What standards and legislation should I be aware of?

In order to effectively implement a security framework it is important to understand what legislation and standards apply today and in the future

Whatever type of organisation or industry you belong to, the laws regarding security and privacy affect you. At an organisational level there is a responsibility to make decisions that do not adversely affect your company.

The legislative and standards frameworks have evolved in conjunction with each other. While there is no legislation dealing directly with IT security governance in Australia, there is numerous legislation which broadly outlines the diligence and care an organisation must take to protect its information assets. As a result, standards have been developed in Australia and adopted from internationally, to provide further guidance on a suitable IT security control environment.

Legislation

Organisations, in both public and private sectors, are potentially liable for the acts of their employees. For example, if an employee propagates a virus attack via an email the organisation may be liable for damages if it is found that there was failure to take reasonable care resulting in the damage incurring.

The Corporations Act 2001 imposes a number of legal responsibilities upon company directors, secretaries and "officers" which is broadly defined to cover COOs, CTOs, CIOs and Information Systems Managers. These requirements suggest, as a director or officer, an obligation to uphold due care and diligence.

The Privacy Act 1988 imposes obligations on certain companies on the way they collect, retain, use and disclose personal information. Companies must take reasonable steps to protect the personal information they hold from misuse and loss from unauthorised access, modification or disclosure. This will require that most companies implement appropriate physical and information security systems to ensure that information held is protected.

If an organisation or individual fails to take "reasonable care" causing damages to another person or company, the negligent company may be liable to pay to the other party. However, if reasonable IT security governance measures are in place, including awareness and accountability, negligence may be avoided.

The Australian Law Reform Commission (ALRC) performed an inquiry into the extent to which the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia. In 2009 the full report was handed down, with a number of key recommendations impacting IT security governance, including data breach notification. The Australian Government has provided a First stage response to the report, with the majority of recommendations accepted by the government.

A broad list of current legislation that can impose a number of legal responsibilities upon your company and individuals are listed **Error! Reference source not found.**. Companies should also be aware of any:

- specific state and territory legislation in the jurisdictions in which they operate or serve customers; and

- any international legislative requirements for those organisations that export or have an overseas presence,.

Table 1- Relevant Information Security legislation

Recent Legislation	Who is affected?
Privacy Act 1988 / Privacy Amendment (Private Sector) Act 2000 ALRC Report 108 - For Your Information: Australian Privacy Law and Practice Australian Government's First stage response to ALRC report (released 14 October 2009)	Australian health care providers, Commonwealth government agencies, and large Australian private companies.
State Privacy Legislation: - *Information Privacy Act 2000 (Vic)* - *Invasion of Privacy Act 1971 (QLD)* - *Health Records (Privacy and Access) Act 1997 (ACT)* - *Privacy and Personal Information Protection Act 1998 (NSW)*	Australian health care providers and the Australian public Sector.
Telecommunications Act 1997	Australian Communication and Media Authority (ACMA), and carriers and carriage service providers.
Telecommunications (Interception and Access) Act 1979 Attorney-General's Department Discussion Paper and Exposure Draft Legislation - Computer Network Protection, July 2009	All organisations operating computer networks.
Statutory Corporations (Liability of Directors) Act 1996	All Australian directors of corporations.

In addition to the legislation listed above, critical infrastructure providers should also be aware of other international legislation. While only organisations that export overseas or with an overseas presence may be impacted directly, knowledge of relevant legislation is beneficial as it may drive future changes in Australian legislation. Such legislation includes but is not limited to the *Sarbanes-Oxley Act of 2002* and the *Gramm-Leach-Bliley Act of 1999* in the United States of America, the *Information Technology Act, 2000* (and current discussions on improvements) in India and other relevant legislation across the European Union.

Standards

When defining an IT security governance framework, benefits can be realised by applying elements from a wide variety of local and international standards. In Australia, businesses subject to regulation in the private sector may choose the Standards Australia based framework (e.g. AS/NZS ISO 31000:2009, AS/NZS 8015, etc).

In some cases Government and other regulatory bodies have mandated, or are in the process of mandating publicly operated critical infrastructure sectors with specific standards (e.g. Protective Security Manual and Information Security Manual). While these security standards apply at a state and territory level, they may also cascade to the local government sector such as in the instance of water and sewerage utilities.

The table below lists the range of standards applicable for the implementation of IT security governance for the protection of critical infrastructure within Australia.

Table 2 - Globally recognised standards

Standards Publisher	Summary
ISO17799 / ISO27001 / ISO27002/ AS/NZS17799 – Code of Practice for Information Security Management Standards Australia, International Organization for Standardization	This standard is a globally accepted code of practice for information security management. It is a controls based standard for organisations to manage their information security according to eleven (11) domains: - Information security policy; - Organising 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; and - Compliance.
Prudential Practice Guide Draft - PPG 234 – Management of IT security risk Australian Prudential Regulation Authority	This draft guide "addresses areas where IT security risk management weaknesses continue to be identified as part of APRA's ongoing supervision activities. It is not the intent of this PPG to replace existing industry standards and guidelines. Instead it provides a set of sound principles for safeguarding IT assets by managing risks and implementing appropriate controls." The guide covers: - IT security risk - An overarching framework - Acceptable usage and user awareness - Identification, access and authorisation - Life-cycle management controls - Monitoring and incident management - Security reporting and metrics - Security assurance It is expected that a final version of the guide will be released in late 2009.
CoʙɪT – Control Objectives for IT ISACA	It provides flexible framework for organisations to meet business objectives and quality, financial and security requirements. It defines seven information criteria: - Effectiveness; - Efficiency; - Confidentiality;

Standards Publisher	Summary
	- Integrity; - Availability; - Compliance; and - Reliability of information,
AS/NZS ISO 31000:2009 Standards Australia / SAI Global	Is a risk management standard. It defines a general framework consisting of five major stages: - Stage 1: Establishing the Context - Stage 2: Identifying the Risks - Stage 3: Analysing the Risks - Stage 4: Assessing & Prioritising Risks - Stage 5: Determining Appropriate Controls
AS8015 – Corporate Governance of ICT Standards Australia	Is an Australian standard for corporate governance of information and communication technology (ICT). It provides six guiding governance principles and a model by which organisations can ensure that IT is aligned with their business objectives. The six principles are: - Establish clearly understood responsibilities for ICT; - Plan ICT to best support the organisation; - Acquire ICT validly; - Ensure ICT performs well, whenever required; - Ensure ICT conforms with formal rules; and - Ensure ICT use respects human factors.
Australian Government Protective Security Manual (PSM) Attorney-General's Department	It is the principal means for publishing Australian Government protective security policies, principles, standards and procedures to be followed by all Australian Government agencies for the protection of official resources. The PSM is the Australian Government's top-level framework for physical, information and personnel security.
Australian Government Information Security Manual (ISM) Attorney-General's Department	An Australian standard to provide policies and guidance to Australian Government agencies on how to protect their ICT systems.

Standards Publisher	Summary

Standards Publisher	Summary
NERC Critical Infrastructure Protection standards – Cyber Security CIP-002 through CIP-009 North American Electric Reliability Corporation (NERC)	These standards have been developed to provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System in the United States of America. These standards recognise the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organisations, for services and data. This results in increased risks to these Cyber Assets.
PCI Data Security Standard (PCI DSS) PCI Security Standards Council	This is a set of security standards that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organisations proactively protect customer payment card account data.

Ethics and duty of care

Demonstrating ethical behaviour and social obligations are key to any organisations core competence and fundamental to critical infrastructure industries. Organisations have a social obligation to the protection of its stakeholders and the public in general, these obligations to threats to attacks of terrorism or even environmental incidents.

What questions can you ask?

Senior executives should ask operational management the following questions about data security and protection:

- Have you identified all key elements of "personally identifiable information" or critical customer data that needs to be protected?

- Have you identified all relevant regulations and compliance requirements regarding security of information systems?

- Have you established the appropriate policies, governance and controls to protect information?

- What are the ongoing metrics and key performance indicators that you are using to monitor compliance with established policies and controls?

- How does the company measure up against these metrics?

- Does the organisation's security culture and "tone at the top" reflect what is required by the company?

- Do the key principles and processes support an IT security governance framework including the involvement of key stakeholders in decision-making?

- Do individuals understand their responsibility for violating the organisation's security policies or compromising the security position of the organisation?

What answers do I need to have for the CEO and the Board?

As outlined in the *Board of Directors and CEO Guidance* paper the following questions, which were taken from a variety of references and discussions, have been provided for your reference.

As a practitioner, you need to ensure you are prepared to answer these questions by implementing an effective IT security governance framework.

Accountability

Has the company assigned executive responsibility for IT security governance?

Does the company have clear and separate accountabilities for enterprise-security governance and management activities?

Adequacy

Does the company have an effective program for monitoring its IT security governance controls and associated regulatory risks?

Awareness

Is there an effective tone at the top to drive cultural change?

Do leaders (directors, senior executives, business-unit managers) understand the key enterprise security risks facing the organisation?

Is there evidence that all employees understand the organisation's security policies and procedures as well as the reason they are in place and enforced?

Do business-unit managers understand their responsibility in the execution of these strategies?

Are awareness and education programs in place to ensure that the business gets the most value from enterprise security?

Compliance

What current legislation is directly linked to the organisation's ability to maintain effective IT security governance (e.g. Privacy Act)?

When was the last time the company evaluated its security risks and regulatory requirements?

Is the general auditor or chief audit executive regularly asking "What should you be doing to demonstrate sufficient control and oversight with respect to information security?"

Effectiveness

How do you ensure security breaches do not jeopardise the organisation and its stakeholders or impact their ability to operate?

Are there sufficient and effective measures in place to protect against and evaluate unauthorised data or security information disclosure?

Ethics

What is management doing to ensure the ethical use of information?

Inclusion

How does the business integrate security into all policies?

Has management considered all stakeholders when developing the organisation's security strategy?

Individual Equity

Are all employees effectively engaged to understand their specific role in upholding the organisation's IT security governance framework?

Information Sharing

How do you share appropriate information with peers and governmental entities?

Measurement

Are there metrics in place to monitor and regulate IT security governance activities?

Has the business agreed on objectives and performance metrics for enterprise security that include measurement and regular reporting of the value that it generates?

Perspective / Scope

Is security taken into account when strategic environmental and cultural decisions are made, for example the value of assets, identified risks and adequate control of security impacts and consequences?

Does security management understand business strategies and priorities when making security decisions? (and visa versa)

Response

Is there an effective response strategy to a potential security breach to key stakeholders such as clients, shareholders, vendors and partners?

Risk Management

Has security been identified as a significant or strategic risk in the company's ongoing risk assessment process? Have steps been taken to mitigate that risk?

All of these questions can be answered through the implementation of an effective IT security governance framework as described.

Where to from here?

To achieve what is required, practitioners need to consider the information presented in this report, apply it to their environment and ensure the three main components of an effective IT security governance framework are in place:

1   Principles;

2   Roles & Responsibilities; and

3   Activities.

This should be done using a top-down approach as illustrated in the following figure to ensure all layers of risk are covered.
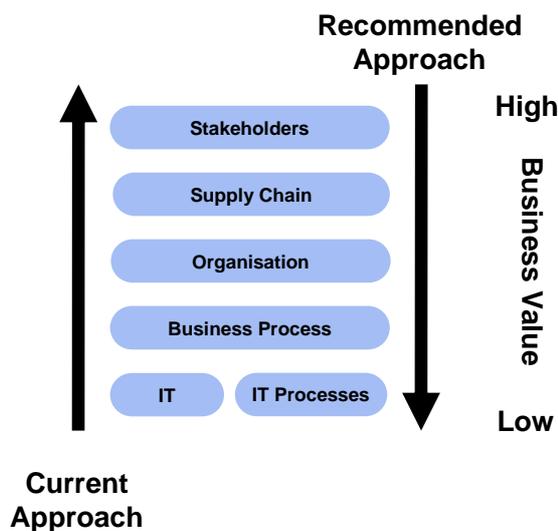

Figure 4 - Approach to implementing IT security governance

In particular, you need to know:

- Stakeholders' expectations for organisation resilience;

- Dependence on the supply chain and the up-stream and down-stream impacts (interdependencies) in the event of an incident;

- The awareness of employees and capability at all levels of the organisation;

- The ongoing effectiveness of controls at the business process layer; and

- The resilience of IT to support business processes.

Board and executive commitment to IT security governance will not ensure its success but a board's lack of commitment will guarantee its failure.

IT security governance should be seen as a business success objective. It is all about what level of risk an organisation and its stakeholders are willing to allow. Every executive needs to understand that it should be addressed with the same logic that is applied to make financial, acquisition and other 'non-security' related business decisions.

To protect Australia's social and economic interests, all organisations – public and private – must take action now to ensure that they are meeting their stakeholders' expectations for IT security and governance, corporate and regulatory compliance and social responsibility. Society's future depends on it.

END OF DOCUMENT