



Trusted Information
Sharing Network
for Critical Infrastructure Protection
.....

**CIO, CISO and Practitioner Guidance
IT Security Governance**

July 2006

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 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 security governance within your organisation. You have an obligation to promote 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 security governance?

While there are many characteristics to security governance, an all-inclusive definition is difficult to contextualise. Leading practice dictates that security governance defines the core 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 security governance was developed and consequently led to the definition to the left.

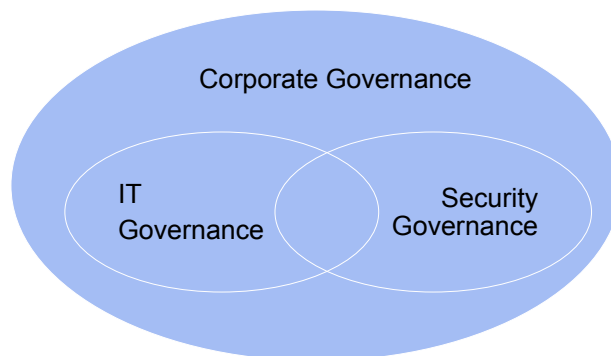


Figure 1: Corporate, IT and security governance relationships

It is important to demonstrate how security governance aligns with the other governing areas that affect organisations. The figure above 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.

Although IT governance and security governance contain a number of similar attributes, their different focus results in an overlap of activities, the distinction ensures security governance framework is not solely driven from an IT point of view.

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

The figure on the following page demonstrates the relationship between security governance and management (operations).

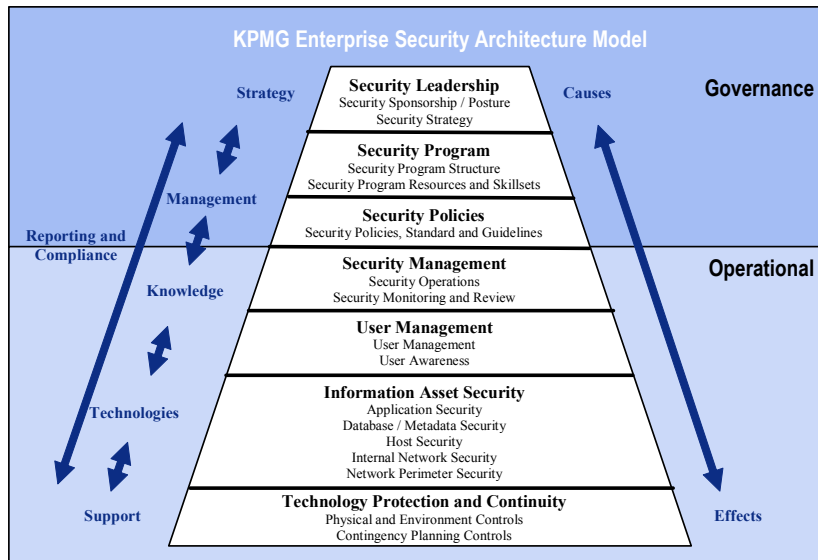


Figure 2: KPMG Enterprise Security Architecture Model

KPMG’s Enterprise Security Architecture Model provides a top-down view of security governance and operations, indicating each of the key focus areas for capability. All layers of the model above are interdependent on one another, thus organisations should ensure that the responsibilities and capabilities of individuals within the organisation adequately cover each layer, and that the linkages between each layer are clearly understood.

A key component of this model, as indicated by the arrows on the left side of the figure, is a reporting and compliance capability that provides monitoring at all levels of the organisation and transparency to the Board regarding the effectiveness of security functions and capabilities. These overarching reporting and compliance functions are critical in supporting the implementation of any security governance framework.

This model has been developed by considering leading practices (such as ISO17799 / ISO27001), as well as practical examples of how leading companies organise their information security functions.

Why is 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 quantifiable impacts of security incidents in Australia have nearly trebled in the last year alone. 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.

Where are we today?

Based upon consultations with key stakeholders in the critical infrastructure community, the following positions summarise security governance in today's environment—in Australia:

- In the absence of local benchmarking, there is a general feeling that the current level of security governance activity (and implementation) in Australia is inadequate. This is supported through a recent Australia National Audit Office (ANAO) report into Internet security in six Australian government agencies which found that the audited agencies did not have security documentation that complied with ICT standards, had limited business continuity planning and inadequate email filtering in place;¹
- Although new standards have been introduced for IT governance (e.g. AS8015 in January 2005), organisations have not yet fully embraced or adopted the recommended practices;
- There is a false sense of security arising from the lack of major incidents in Australia; and
- Critical infrastructure industries are not forced by regulation or legal directives to ensure that effective security governance frameworks and practices are in place.

The result is that while the awareness of the risks has increased, there is still a lot of work to be done.

Threats and drivers

With the risks and threats to IT security dynamically changing, owners and operators of critical infrastructure require strong security governance to ensure effective ongoing management of risk.

The following list, which is not intended to be considered all-inclusive, represents categories that have been identified as the greatest threat to critical infrastructure industries:

Human error: can be considered inevitable but the number of incidents related to human error can be prevented and reduced considerably with effective governance. This category also includes people's failure to act, and their lack of accountability.

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.

Malicious software: viruses, worms and spyware, are 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 placed in the corner and left alone; they are just as susceptible to attack as any other network based system.

¹ Crawford, M., 15 June 2006, *Nairn disappointed with ANAO report: launches workgroup*, www.computerworld.com.au

Table 1: Total annual cyber crime losses, below, has been drawn from the conclusions of the 2006 Australian Computer Crime and Security Survey² and demonstrates that even though the number (volume) of successful attacks have decreased in recent times, their impacts can be catastrophic from a financial perspective.

Total annual loss (\$)				
	2003	2004	2005	2006
Total	11 800 783	15 921 064	16 856 900	48 471 208
Average	93 657	116 212	153 245	241 150

Table 1: Total annual cyber crime losses

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, it is just a matter of time before most Australian organisations become a part of the statistics.

What do you need to know?

Figure 3: Security governance framework outlines the responsibilities for key executive roles and for employees as a whole to achieve the level of accountability necessary for effective security governance at an enterprise level.

This figure illustrates an example of a leading practice model that incorporates the external and internal interactions required to operate an organisational security governance function. Key to any organisation (in both public and private sectors) is the security governance activities that foster and maintain a sustainable and controlled security function that meets the organisational objectives and strategy.

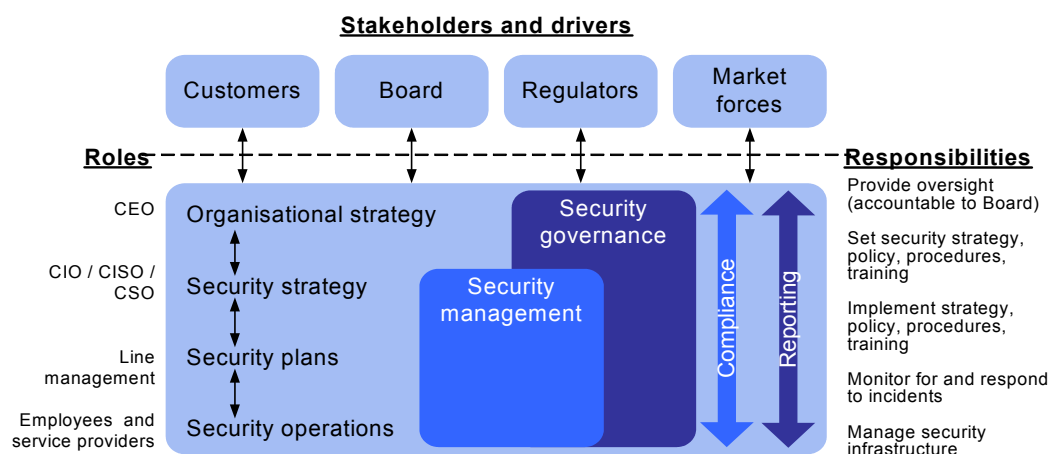


Figure 3: Security governance framework

Why do I need executive buy-in?

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

² AusCERT 2006, *Computer Crime and Security Survey*, Author, Brisbane.

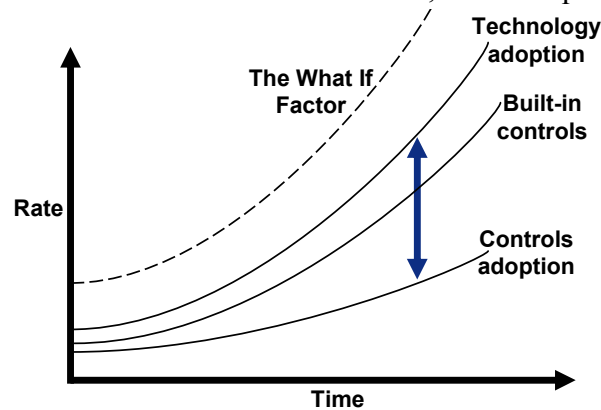
Security governance should be seen as a business success objective. It is all about what level of risk an organisation and its stakeholders are willing to accept. Every executive needs to understand that it should be addressed with the same logic that is applied to make financial, acquisition and other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

What do your stakeholders expect from you?

Stakeholders including board executives, need to trust in an organisation's diligent protection of its information, including privacy and identity, and assets.

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

- 1 Provide guidelines for accepted 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 the implementation, monitoring and review of security (security strategy) including alignment to legislative and best practice standards; and
- 7 Ensure internal and external audits occur, with adequate plans in place to



remediate findings.

Figure 4 - IT adoption vs. controls adoption

What are the risks to my organisation?

The risks are increasing to society, economy and ultimately the industry's ability to meet stakeholder expectations are ever increasing. 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.

The arrow on the graph highlights the increasing gap and resulting increased opportunity for risk as described.

Leading practices demonstrate that security governance and management activities should be driven from a risk management point of view.

What standards and legislation should you be aware of?

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.

Standards

When defining a 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 4360, AS/NZS 8015, etc).

In some cases 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 ACSI 33). 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 security governance for the protection of critical infrastructure within Australia.

Standards	Summary
Publisher	
<p>ISO17799 / ISO27001 / AS/NZS17799— Code of Practice for Information Security Management</p> <p>Standards Australia, International Organization for Standardization</p>	<p>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 11 domains:</p> <ul style="list-style-type: none"> • 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.
<p>COBIT—Control Objectives for IT</p> <p>ISACA</p>	<p>It provides flexible framework for organisations to meet business objectives and quality, financial and security requirements. It defines seven information criteria:</p> <ul style="list-style-type: none"> • Effectiveness; • Efficiency; • Confidentiality; • Integrity;

Standards	Summary
Publisher	
	<ul style="list-style-type: none"> • Availability; • Compliance; and • Reliability of information.
<p>AS/NZS 4360:1999—Risk Management</p> <p>Standards Australia / SAI Global</p>	<p>Is a risk management standard. It defines a general framework consisting of five major stages:</p> <ul style="list-style-type: none"> • 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
<p>AS8015—Corporate Governance of ICT</p> <p>Standards Australia</p>	<p>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:</p> <ul style="list-style-type: none"> • 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.
<p>Australian Government Protective Security Manual (PSM)</p> <p>Protective Security Coordination Centre (PSCC)</p>	<p>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.</p>
<p>ACSI 33—Australian Government Information and Communications Technology Security Manual</p> <p>Defence Signals Directorate (DSD)</p>	<p>Is an Australian standard to provide policies and guidance to Australian Government agencies on how to protect their ICT systems?</p>
<p>FERC/NERC Urgent Action Standard 1200—Cyber Security</p> <p>The Federal Energy Regulatory Commission (FERC)</p>	<p>Is a standard that is designed to safeguard the industry and its customers against these risks through vulnerability assessments, threat response strategies, emergency management planning, employee background checks, physical and communications fortifications, and other measures a prescriptive approach that can help compliant companies:</p> <ul style="list-style-type: none"> • Demonstrate a serious security commitment to customers, partners and regulatory agencies;

Standards	Summary
Publisher	
and the North American Electric Reliability Council (NERC)	<ul style="list-style-type: none"> • Prioritise spending; • Enable integration and scalability; • Reduce operational risk; • Establish a focused framework for compliance audits; and • Improve overall corporate stability.

Table 2: Globally recognised standards

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 security governance measures are in place, including awareness and accountability, negligence may be avoided.

A broad list of current legislation that can impose a number of legal responsibilities upon your company and individuals are listed below:

Recent Legislation	Who is affected?
Privacy Act 1988 / Privacy Amendment (Private Sector) Act 2000	Australian health care providers, Commonwealth government agencies, and large Australian private companies.
State Privacy Legislation: <ul style="list-style-type: none"> • 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 	Australian health care providers and the Australian public Sector.

Recent Legislation	Who is affected?
1998 (NSW)	
Telecommunications Act 1997	Australian Communication and Media Authority (ACMA), and carriers and carriage service providers.
Statutory Corporations (Liability of Directors) Act 1996	All Australian directors of corporations.
US Sarbanes-Oxley Act of 2002	All public companies subject to US security laws.
US Gramm-Leach-Bliley Act of 1999	US Financial institutions.
US Health Insurance Privacy and Accountability Act (HIPAA)	US Health plans, health care clearinghouses, and health care providers.
Senate Bill 1386 (SB1386), California, USA	US California agencies, persons and businesses that conduct business in the State of California.
US Federal Information Security Management Act (FISMA)	US Federal agencies.

Table 3: Relevant Information Security legislation

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 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.

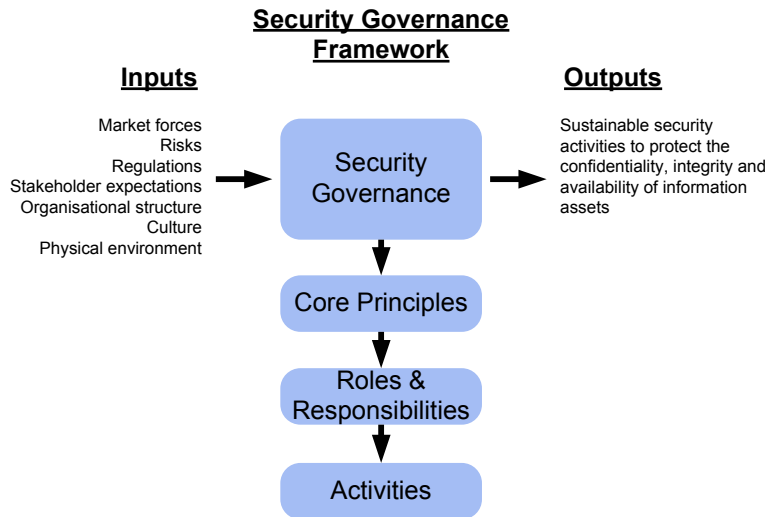


Figure 5:- Leading practice security governance framework

This framework is composed of three components:

- 1 **Core principles:** Serve as the primary driver for all 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 security governance activities take place and achieve the spirit of the core principles. 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 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 security governance within a corporate governance environment.
- 3 **Activities:** The underlying processes that are owned and operated by accountable individuals to implement and maintain 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;
- Implement and maintain policies and procedures based on risk assessments to secure its information and assets based on industry sound practice. ISO17799 describes one such standard which can be used to do this. This standard covers eleven core domains as follows:
 - 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 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 a 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 security governance framework.

Accountability

Has the company assigned executive responsibility for 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 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 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 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 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 security governance framework as described.

Where to from here?

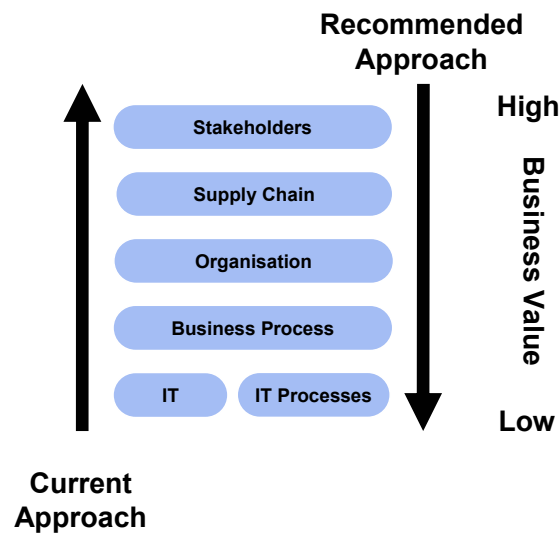
To achieve what is required, practitioners need to consider the information presented in this report, apply it to their environment and ensure the three main components of an effective security governance framework are in place:

- 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.

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.

Figure 6: Approach to implementing security governance

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

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.