Trusted Information Sharing Network
for Critical Infrastructure Protection

Secure Your Information:

Information Security Principles for Enterprise Architecture

Report

June 2007

DISCLAIMER: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgment of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs. This report was prepared by SIFT Pty.Ltd. for the Department of Communications, Information Technology and the Arts on behalf of the Information Technology Security Expert Advisory Group.

Foreword

Rapid development in information and communication technologies and the changing business environment present a range of challenges for organisations that rely on such technologies for day-to-day operations. Critical infrastructure sectors are at particular risk from interruption to information technology operations as this can lead to major economic and social disruption. As a result, it is vital for owners and operators of critical infrastructure to develop appropriate strategies for mapping and understanding the layers of information held on IT networks that need to be protected.

The Department of Communications, Information Technology and the Arts (DCITA), on behalf of the IT Security Expert Advisory Group (ITSEAG[*]) of the Trusted Information Sharing Network (TISN[†]), engaged SIFT Pty. Ltd. to produce a report and supplementary guidance regarding enterprise strategy for information security for owners and operators of critical infrastructure. The *Secure Your Information* set of papers are the result of this project.

The TISN has previously released a series of papers to help CEOs and Boards of Directors understand threats to their IT infrastructure, and to provide recommendations for mitigating those threats. Issues covered in these documents range from Managing Denial of Service Risks to IT Security Governance. These papers are available at: *www.tisn.gov.au*.

This paper is closely related to the *Leading Practices and Guidelines for Enterprise Security Governance* report, which was developed to provide guidance for the implementation of information security governance structures within an organisation.

The Governance paper highlighted the growing gap between the speed of technology adoption and of security control implementation. The governance framework provides strategies for achieving strong security governance given the challenges of the modern business environment.

This paper is related to the Governance paper by the inclusion of a set of core information security principles which can be used by an organisation's decision makers to plan and develop security around information assets within changing Enterprise Architectures. The techniques and frameworks discussed in the Governance paper provide a valuable mechanism for ensuring the principles are effectively adopted.

In developing this work, SIFT (*www.sift.com.au*) engaged in discussions with members of the ITSEAG and other relevant bodies including key stakeholders from the IT and information security sectors and owners and operators of critical infrastructure to gain an individual industry perspective on the issues. SIFT thanks all participants for their contributions to the project.

---

[*] The ITSEAG is one of three Expert Advisory Groups established within the Trusted Sharing Information Network for Critical Infrastructure Protection. The ITSEAG provides advice to the Critical Infrastructure Advisory Council (CIAC) and the sector based Information Assurance Advisory Groups on IT security issues as they relate to critical infrastructure protection. The ITSEAG membership consists of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security fields.

[†] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups, three Expert Advisory Groups, and the Critical Infrastructure Advisory Council (CIAC—the peak body of TISN that oversees the IAAGs and EAGs). More on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au.

Contents

Figures

Tables

Case Studies

Technical Studies

Executive Summary

Directors and Officers are ultimately responsible for protecting enterprise information (both physical and electronic) against unauthorised access or damage—whether malicious or accidental. The security of information is vital operationally, legally and financially. Failure to address security requirements can have serious consequences, including long term damage to reputation, especially for organisations underpinning the nation's critical infrastructure. Financial consequences of breaches can also be significant. Total losses recorded in the 2006 Australian Computer Crime and Security Survey were more than AU$48 million—an average of $241 150 per organisation[1]. Similarly, the 2006 CSI / FBI Computer Crime and Security Survey reported average losses of over US$167 700 per organisation[2].

The security of Australia's critical infrastructure has a direct relationship to our national security. In 2006, the Attorney-General Philip Ruddock noted that information security is "crucial in meeting the broader security challenge". He highlighted the need for critical infrastructure organisations to embrace a best practice based approach[3].

While the approach to information security may vary between organisations due to a difference in resources and business objectives[4], there is an underlying set of requirements that all organisations must follow in order to ensure the security of their information assets. This paper defines **Seven Basic Principles of Information Security** that must underpin the enterprise's strategy for protecting and securing its information assets:

1. *Information Security Is Integral to Enterprise Strategy*
2. *Information Security Impacts on the Entire Organisation*
3. *Enterprise Risk Management Defines Information Security Requirements*
4. *Information Security Accountabilities Should be Defined and Acknowledged*
5. *Information Security Must Consider Internal and External Stakeholders*
6. *Information Security Requires Understanding and Commitment*
7. *Information Security Requires Continual Improvement*

These principles have been developed in line with global and national information security best practice and have been thoroughly reviewed and endorsed by the Australian IT Security Experts Advisory Group (ITSEAG*). They are intended to allow organisations to better meet their obligations in achieving corporate governance requirements for information security, including legal and regulatory compliance.

---

[1] AusCERT, *Computer Crime and Security Survey*, 2006, *http://www.auscert.org.au/images/ACCSS2006.pdf*

[2] Computer Security Institute, *CSI/FBI Computer Crime and Security Survey*, 2006, *http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf*

[3] S Grose, *'Federal Government to Toughen Information Security', ZDNet Australia*, 2006, *http://www.zdnet.com.au/news/security/soa/Federal-government-to-toughen-information-security/0,130061744,139249593,00.htm*

[4] G Wang *'Strategies and Influence for Information Security', Information System Control Journal, vol 1, 2005*, Information Systems Audit and Control Association

The principles are relevant across all industry sectors for the design, development and maintenance of a secure enterprise strategy and architecture. Implementing these principles throughout the organisation will give management the confidence to accept the responsibility of protecting the organisation's information assets in today's dynamically changing environment – a key objective in information security governance[5]. In particular, understanding the principles and incorporating them throughout the organisation's system lifecycle is a vital aspect of the overall information security management scheme.

When everyone in the enterprise integrates these principles into their daily activities, either by planning the strategic direction of the organisation or simply running its day to day operations, a 'culture of security' will develop that will support the ongoing integrity of the organisation's information assets, as well as supporting the legal and regulatory compliance obligations demanded of the organisation.

Organisations today are facing constant and often profound change—from the marketplace, competitors, advancing technologies, and growing client expectations[6]. Global changes such as corporate governance reform, security concerns arising from terrorism, and increased malicious Internet activity have required organisations to be resilient in times of competition and uncertainty.

Convergence of Enterprise Architecture

In order to adapt to this environment, organisational design needs to be reconsidered. Enterprise Architecture—the formal description and detailed plan of an organisation—needs to be flexible enough to cope. The challenge for many organisations has been achieving a flexible user-oriented architecture while maintaining a 'culture of security'.

---

[5] ITSEAG (Trusted Information Sharing Network), *Leading Practices and Guidelines for Enterprise Security Governance*, 2006, *http://www.dcita.gov.au/__data/assets/pdf_file/41308/IT_Security__and__Governance.pdf*

[6] L Friedman & H Gyr, *'Business Strategy Tools for OD Practitioners: Creating the Dynamic Enterprise, Vision/Action Journal of the Bay Area OD Network'*, 1998

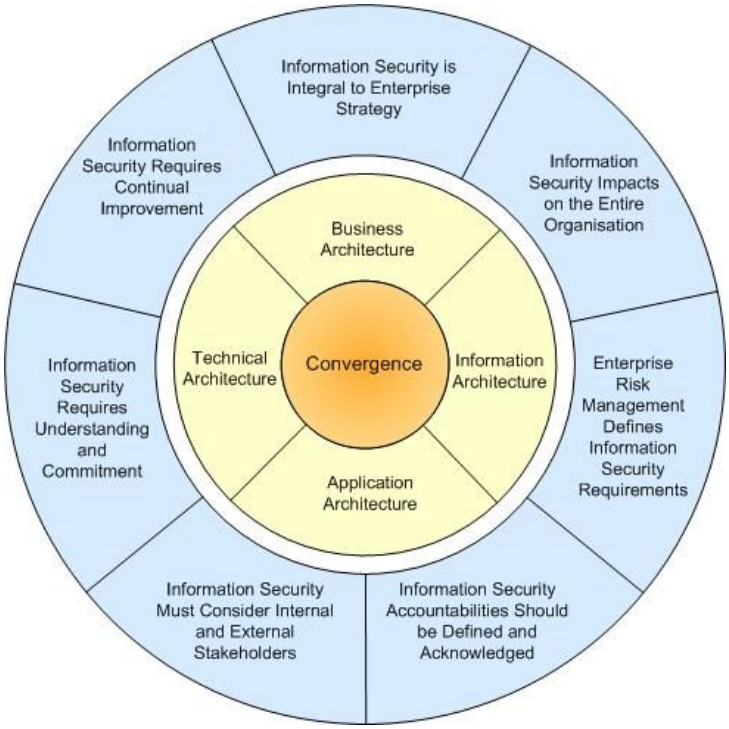
A particular challenge for Enterprise Architecture today is convergence: the integration of elements and functionalities within the Enterprise Architecture, including:

- Centralisation of business functions;
- An increasing interconnectedness of organisations through shared networks;
- Deployment of service oriented architectures (SOA);
- Simplification of applications through the use of ubiquitous web interfaces;
- Integration of voice and data networks on single infrastructures; and
- Wide deployment of multifunctional handheld and network devices.

Convergence affords organisations with benefits including operational efficiencies, increased speed to market, improved customer service and a quicker return on investment. However, the removal of security barriers from previously strictly defined and separated organisational structures presents significant challenges including:

- Potential degradation in quality of service over shared infrastructure;
- Issues associated with distribution of and added complexity to authentication and authorisation mechanisms;
- Increased points through which systems and organisations can be attacked;
- Increased confusion about where and to whom responsibility and accountability apply; and
- Incident detection and response issues in interconnected environments with many external parties.

Critical business information now exists extensively on laptops, personal digital assistants (PDAs), USB keys and portable hard drives, components which often exist outside the traditional definition of the organisation's secure perimeter. This perimeter is changing to include customers, suppliers, business partners, and the mobile workforce, creating a new 'mobile perimeter' that increases enterprise risk. In order to manage the secure evolution of this perimeter, the adoption of an enterprise wide, strategic approach to information security is critical.



Relationship between Principles of Information Security, Enterprise Architecture and Convergence

In this environment, protecting enterprise information (both physical and electronic) from leakage, accidental or malicious destruction, and illicit change has become increasingly difficult. It is necessary to develop an effective governance framework to manage security risks and distribute responsibility.

In meeting these contemporary challenges, The IT Security Expert Advisory Group* of the Trusted Information Sharing Network† has developed this resource which includes:

- Seven key information security principles (as noted above and illustrated in the outer ring in the image above) for developing an enterprise strategy for information security;
- Approaches for linking these seven key information security principles to your enterprise architecture (as shown by the inner ring in the image above);
- Recommendations for information security to ensure the integration of security controls throughout the categories of ‘people, process and technology’; and
- A self-assessment Checklist for validating an enterprise strategy for information security.

The principles presented provide a set of key requirements to be considered in order to ensure information security considerations are addressed within the organisation, and in the context of Enterprise Architecture.

Each principle includes a set of recommendations which should be used to apply the principles throughout an organisation. Case studies are used to illustrate the application of these recommendations in practical scenarios relevant to critical infrastructure organisations.

Following the principles and their recommendations, the paper works through the application of the principles in the context of Enterprise Architecture. The paper applies the recommendations outlined to the process of Security Architecture Development by tracing the

phases of one popular Enterprise Architecture development process. At each phase, relevant considerations of the principles of information security are discussed along with practical examples of the principle usage.

Technical case studies based on convergence are used to illustrate the application of principles through contemporary examples of architectural change. These are framed within many of the architecture components discussed, including:

- Business Architecture;
- Information Systems Architecture (Data and Application Architecture);
- Technology Architecture (Technical Architecture); and
- Architecture Change Management.

While convergence is changing the information landscape for critical infrastructure organisations, the underlying principles used to ensure the security of this information are largely unchanged. As the effects of convergence become more apparent, the use of “first principles” as detailed in this paper can ensure security architecture remains enforceable, measurable and continues to adequately protect the organisation.

Overview

Structure of the report

The overview section of this paper provides the business and technology context in which enterprise strategy for information security is created. The following two sections of the paper can be reviewed independently.

The first section entitled 'Principles of Information Security' presents each principle with a set of best-practice recommendations which can be applied to implement the principle throughout the organisation. In turn, each recommendation presents a number of action items which illustrate specifically how the recommendations can be implemented (Figure 1).

Figure 1: Principles of information security structure

This section also examines a number of case studies within its recommendations in order to provide a real-life view of how the principles have been applied, or where the principles can be used to identify how an issue would have been avoided.

The second section entitled "Security Architecture Development" applies the information security principles within the context of Enterprise Architecture development. Recommendations from the principles are applied specifically to Enterprise Architecture components as part of each phase of *The Open Group Architecture Framework (TOGAF)*[7] Architecture Development Method (ADM)—a reference process defined for the development of Enterprise Architecture—to demonstrate how a Security Architecture[8] can be developed. The use of TOGAF ADM in this report is illustrative, and considerations identified in this section apply equally to most Enterprise Architecture methodologies.

A number of technical studies are then provided to demonstrate how the challenges of convergence can be handled at various architecture layers (Figure 2).

Figure 2: Security Architecture Structure

Appendices are provided for the reader's reference including a checklist of action items that can be used to verify an organisation's compliance with security principles.

[7] The Open Group, *TOGAF (The Open Group Architecture Framework) Enterprise Edition, Version 8.1*, 2003, *http://www.opengroup.org/architecture/togaf8-doc/arch/*

[8] The Open Group, *Guide to Security Architecture in TOGAF Architecture Development Method (ADM)*, 2005, *http://www.opengroup.org/architecture/togaf8-doc/arch/chap03.html*

Critical Infrastructure

The Attorney-General's Department of the Australian Government has defined critical infrastructure as

"Those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security"[9].

In this context, the following industries are considered by this paper, with utilities and telecommunications providing the underpinning support services.

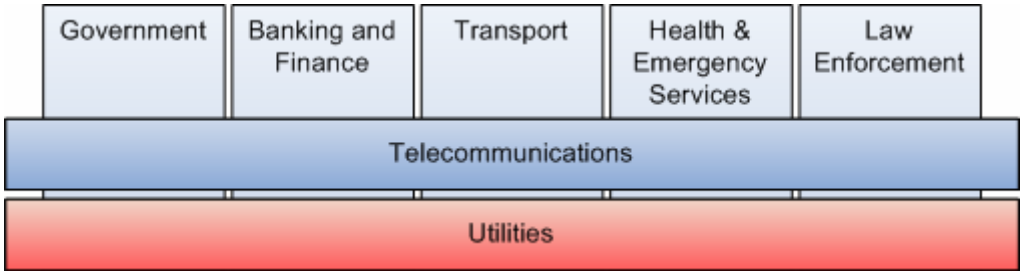


Figure 3: Critical Infrastructure Industries[10]

Australia's socio-economic wellbeing is directly affected by the availability of services from critical infrastructure organisations. Thus critical infrastructure organisations have a responsibility to the Australian community to manage the threat of impacts to availability[10] as well as overall system integrity and required confidentiality. This extends to managing the overall security of information assets which assist in enabling the organisation to operate.

In 2006, the Attorney General Philip Ruddock indicated that information security is "crucial in meeting the broader security challenge" and highlighted the need for critical infrastructure organisations to embrace a best practice and standards based approach for information security particularly given that up to 90 percent of critical infrastructure in some Australian areas is in private hands[3].

Consequently, a principles based approach developed in line with existing national and international best practices for information security is developed in this report to aid these organisations in incorporating security into their Enterprise Architecture design, development and maintenance.

While application of these principles may vary from organisation to organisation, and industry to industry, these principles and their recommendations form a baseline which allow critical infrastructure organisations to structure their information security governance program to ensure information security risks are consistently and appropriately addressed.

---

[9] Attorney-General's Department, *Trusted Information Sharing Network: About Critical Infrastructure*, 2006, *http://www.tisn.gov.au/*

[10] Trusted Information Sharing Network, *Denial of Service / Distributed Denial of Service – Managing DoS Attacks*, 2006, *http://www.dcita.gov.au/__data/assets/pdf_file/41312/DoS_Report.pdf*

Enterprise Strategy

In order to successfully implement information security in an organisation, management must include information security within the organisation's strategy, planning and structure. Information security strategy cannot exist by itself, apart from the rest of the organisation. To be truly effective information security objectives must become a normal part of day to day operations and must be built into the strategic planning process. This report provides a set of Principles of Information Security which, when built into the organisation's governance processes, enables the development of an organisational security culture.

An effective enterprise strategy allows organisations to create a unique and valuable market position[4]. Business strategy is used to outline the progressive direction an organisation intends to take in order to achieve its mission. The business strategy incorporates both short and long term planning of the organisation's business activities[11].

In order to understand the scope of enterprise strategy—and hence the required approach to defining an enterprise strategy for information security—it is important to consider the layers of strategy within an organisation.

- Enterprise strategy is the top level directive which includes the overarching goals for the organisation. This provides a foundation for the organisation's strategic business units or divisions to develop individual functional or operational strategies.
- Functional strategies are those specific to individual strategic business units. These strategies translate the enterprise strategy to specific short to medium term objectives which are applicable to the unit alone.
- Operational strategies are influenced by the functional strategy. These are the lowest level and focus on day-to-day operational activities.

Figure 4: Enterprise Strategy Structure

[11] UM Stroh, *An Experimental Study of Organisational Change and Communication Management*, 2005, Faculty of Economics and Management Sciences, University of Pretoria

The Internet age has brought about a change in the way organisations conduct business and has significantly influenced all aspects of enterprise strategy. The most notable changes include[12]:

- Globalisation—the globalisation of the economy has introduced new audiences for products and services while forcing organisations to break down international borders in search of a lower cost of labour.
- Quicker time to market—the opportunity to adopt innovative technology at a quicker pace which can create a knowledge gap in the ability of the organisation to effectively deploy these technologies.
- Changing business relationship structures—the development of new inter-organisational alliance and partnership structures that are shorter in horizon and greater in scope.
- Mobile workforce—employees are less willing to commit to their jobs long term, and are often required to work in non-conventional environments with flexible arrangements.

Furthermore, global changes such as corporate governance reform and security concerns arising from terrorism have required organisations to be resilient in times of competition and uncertainty. As a result, the concept of "dynamic strategy" has developed in response to the need to continually evolve the enterprise strategy to fit changing times.

The shifting economic environment has dictated a shift in focus from production agents being recognised as the organisation's critical assets, to information as the critical and differentiating asset. Information technology systems have allowed organisations to create centralised knowledge management systems affording the ability for departments to share information and achieve common objectives more readily.

Enterprise Architecture

This shift in the approach towards dynamic enterprise strategy has given rise to the need to rethink the structure of organisations to enhance flexibility, scalability and adaptability. In other words, frameworks for developing and maintaining the organisation's Enterprise Architecture must seek to address these strategic objectives on an ongoing basis. The challenge is to cope with change whilst ensuring information assets which provide competitive advantage are securely maintained.

Formally, Enterprise Architecture is the description or detailed plan of an organisation, its components, their interrelationships, and the principles governing their design. Any enterprise strategy for information security must therefore be considered in the context of the organisation's Enterprise Architecture. Attempting to implement security as an afterthought to Enterprise Architecture is likely to fail and it must therefore be 'designed-in' as part of the Enterprise Architecture process.

The Open Group Architecture Framework (TOGAF)[7] defines the four fundamental components of Enterprise Architecture (presented in Figure 5). The Business Architecture must be the first component to be analysed and defined as the results of this feed into the lower layers as requirements. Varying approaches to the development order of Data and Application Architecture exist due to their inter-reliance, hence they are sometimes considered together as 'Information Systems Architecture', as illustrated in Figure 5.

---

[12] DL Pipkin, *Information Security – Protecting the Global Enterprise,* 2000, HP Professional Series

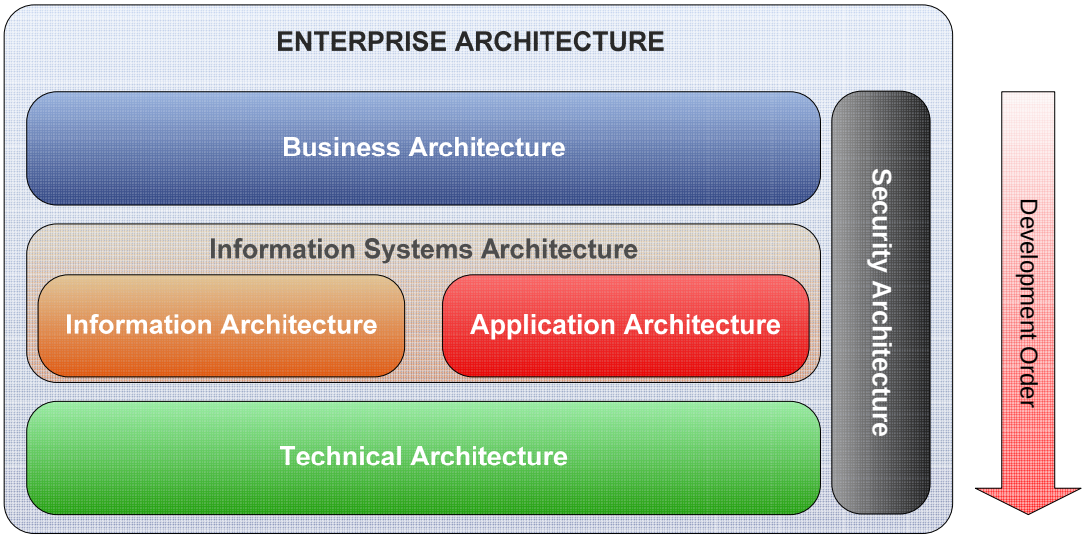


Figure 5: Enterprise Architecture Components

The four components are as follows:

- **Business Architecture**

Business Architecture is the set of tangible and intangible assets representing business strategy, governance, and key business processes. It includes the over-arching description of organisational mission, goals and functions, as well as employee roles and responsibilities.

- **Information Architecture (sometimes referred to as 'Data Architecture')**

Information Architecture is closely related to Application Architecture, and the two together are known as 'Information Systems Architecture'. Information Architecture is the set of tangible and intangible assets representing logical and physical data assets, and data management resources required for the successful operation of the organisation.

- **Application Architecture**

Application Architecture is closely related to Information Architecture, and the two together are known as 'Information Systems Architecture'. Application Architecture is the set of tangible and intangible assets representing the applications required to support business processes, including their interactions and relationships.

- **Technical Architecture (sometimes referred to as 'Technology Architecture')**

Technical Architecture is the set of tangible and intangible assets representing the software and hardware required to support Information and Application Architectures.

In addition to the four key components of the TOGAF Enterprise Architecture model, a "vertical" architectural stream exists to ensure that security is applied effectively and consistently throughout the layers. This is a critical component for the effective functioning of the Enterprise Architecture.

- **Security Architecture**

Security Architecture is the set of tangible and intangible assets representing security controls and mechanisms within the Enterprise Architecture. Security Architecture is integrated throughout the four Enterprise Architecture components. Furthermore, it is integrated into the

architecture development cycle (described in the Security Architecture Development section of this report) and results in additional requirements being identified during each stage of the development. A critical component of the Security Architecture is Security Governance.

While other Enterprise Architecture frameworks and development methods exist such as the Zachman Framework[13], and the US Department of Defense Architecture Framework (DoDAF)[14], the issues and examples discussed are equally applicable to these. This is due to the common approach to separating architecture components and the requirement to conduct pre and post-architectural activities. Furthermore, the effectiveness of the recommended security controls does not change between frameworks.

Developing an Enterprise Architecture and therefore a Security Architecture is a cyclical process (as shown by Figure 11 in the Security Architecture Development section of this report). It starts with the definition of a baseline architecture that states the organisation's current position including consideration of external requirements. From this, a target architecture which the organisation aims to achieve is created. During architecture migration—from the baseline architecture to the target architecture—a number of intermediate or transition states are encountered.

Convergence

A key factor in the development of the modern discipline known as Enterprise Architecture is the concept of convergence. Convergence describes the merging of elements and functionalities within the Enterprise Architecture. Without the enhanced use of technology that convergence enables, many of the strategies defined in today's enterprise architectures would be unworkable.

Recent prominent architectural changes resulting from convergence include:

- Centralisation of business functions (e.g. A single human resources team serving an entire economic region);
- Creation of geographically dispersed self-managed project teams;
- Interconnection of organisations through shared networks;
- Deployment of Service Oriented Architectures (SOA—an information systems design based on loosely coupled software services built to support seamless business process interactions.)[15;]
- Simplification of applications through the use of ubiquitous web interfaces;
- Integration of voice and data networks on flexible infrastructures; and
- Development and deployment of multifunctional handheld and network devices.

---

[13] The Zachman Institute for Framework Advancement, *Zachman Framework Definition,* 2007, *http://www.zifa.com/quickstart.html*

[14] The United States Department of Defense, *Enterprise Architecture,* 2007, *http://www.defenselink.mil/cio-nii/cio/earch.shtml*

[15] MSDN, *Service Oriented Architecture,* 2007, *http://msdn2.microsoft.com/en-us/architecture/aa948857.aspx*

The primary drivers for convergence are the need for organisations to seek:[16]

- Operational efficiencies due to unification of multiple networks and potential ability to scale at a lower cost;
- Increased speed to market and rapid launch of new services by leveraging open standards and existing infrastructure;
- Improved customer service by providing the ability to conduct self-management and lessening the burden on support services; and
- Quicker return on investment due to reduced operational overhead.

Figure 6: Convergence of Enterprise Architecture

Convergence, while delivering benefits to productivity, has weakened the security controls in place in the formerly compartmentalised structures. Convergence has introduced challenges to enterprise strategy for information security including:

- **Unauthorised functionality**

Devices now perform functions in excess of business requirements. The use of such functions may be difficult to control and may be abused for unauthorised access.

- **Availability of service**

Different business processes sharing a single infrastructure often require different quality of service levels. Similarly, a single process can require quality of service across infrastructure managed by multiple organisations. Potential exists in these situations for competing objectives to cause a degradation of quality or even denial of service.

- **Confidentiality, integrity, and privacy**

Different business processes sharing a single infrastructure may transport information of different security levels and will therefore require differing levels of confidentiality and

[16] Verisign, *Building a Security Framework for Delivery of Next Generation Network Services*, 2005, *http://www.verisign.com/static/035478.pdf*

integrity to be maintained. Furthermore, even information at the same security level must often not be revealed to other business processes to maintain privacy.

- **Authentication and authorisation**

The more dispersed the user base of a system and the greater the number of system components which provide authentication and authorisation, the greater the complexity and effort required to provide those services uniformly throughout the organisation.

- **Increased attack surface**

Convergence causes system and network perimeters to be extended to other system components and even organisations. As the perimeter is extended the number of potential attackers and potential points subject to attack, increases rapidly.

- **Responsibility and accountability**

As business boundaries are blurred, the responsibility for maintaining security of shared infrastructure can become unclear. Moreover, in the event of a security incident, the transient responsibility for connected peer security brings about accountability issues.

- **Incident detection and response**

The detection and response function comprises a significant proportion of operational security. When security requirements cross organisational boundaries or shared infrastructure, detecting an incident, identifying the source, and preventing further attack can be logistically and operationally difficult to co-ordinate.

Appendix A shows a mapping of the Principles of Information Security introduced in this report and their ability to address these convergence challenges. Specific convergence scenarios and technologies are covered in the Security Architecture Development section of this report. Effectively applying the Principles of Information Security will ensure that security risks introduced by convergence are appropriately identified and mitigated.

Information Security

Information security is the protection of information and information systems. It encompasses all infrastructure that facilitates its use—processes, systems, services and technology[17].

Information Security vs. IT Security

Information security is the protection of information and information systems. It encompasses all infrastructure that facilitate its use – processes, systems, services and technology.

IT security is a subset of information security and is concerned with the security of electronic systems, including computer, voice and data networks.

Source: Australian National Audit Office[17]

[17] Australian National Audit Office, *IT Security Management Audit Report No.23 2005-2006,* 2005, *www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf*

The discipline of information security has itself been subject to the forces of convergence. Information technology (IT) security is the discipline of providing technical controls around IT systems which guard against unauthorised access, use, disclosure, destruction, modification or disruption of access to data. IT security therefore is a subset of information security in that it aids the information security process by ensuring protection of information enabling IT systems are protected.

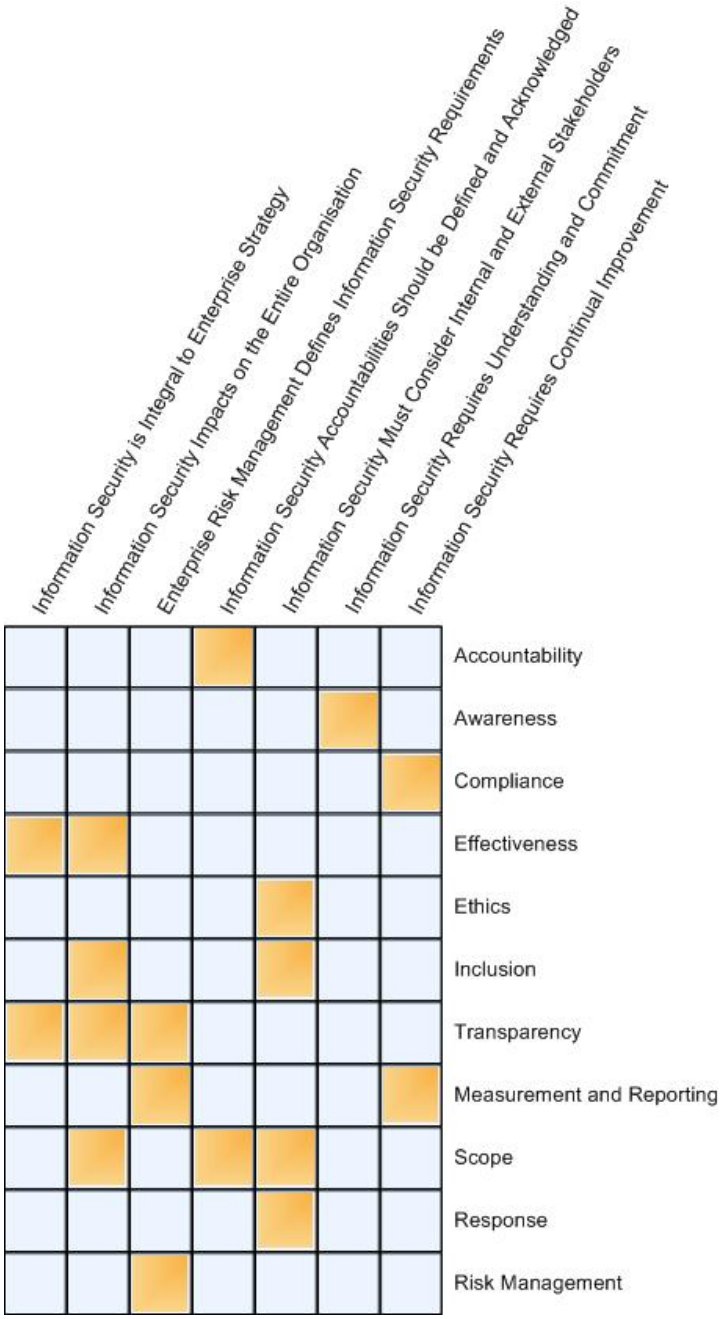


Figure 7: Mapping Enterprise security principles to TISN Governance security principles

For IT security to be effective in protecting the interest of the organisation, it must be aligned with physical and personnel security practices of the organisation. This unified approach is the practice of information security at its core.

Information Security Governance

A key strategic challenge for organisations today is meeting corporate governance compliance requirements while maintaining a dynamic and innovative enterprise. A prudent information security governance program assists organisations to positively monitor the protection of stakeholder information and interests while balancing risk, cost and service.

Information security governance is therefore considered a subset of corporate governance. It is the process of establishing and maintaining a framework, supporting management structures and processes to provide assurance that information security strategies are aligned with and support business objectives[18]. A successful governance program enables the organisation to effectively manage security during periods of change. A successful governance framework is essential for the development of a 'culture of security'[19] within the enterprise[5].

TISN released a paper in July 2006, entitled *Leading Practices and Guidelines for Enterprise Security Governance* which provides a guideline for implementing information security governance structures within an organisation. The paper explains that a successful governance structure must define key security principles, accountabilities and actions which an organisation must follow to ensure their objectives are achieved. The *Secure Your Information* paper (this paper) ties in to this governance work by providing the principles which organisations can use to form a basis for development of policies and systems dictating organisational security accountabilities and actions[5]. In Figure 7 shown above, the principles identified in the July 2006 paper are mapped to the principles in this paper.

The Governance paper also highlights the growing gap between the speed of technology adoption and that of security control implementation. The governance framework provides a number of strategies for achieving strong security governance given this gap.

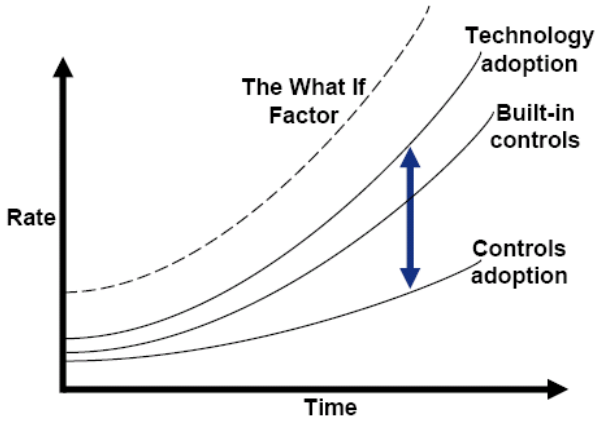


Figure 8: IT Adoption vs Controls Adoption

[18] The United States National Institute of Standards and Technology, *Information Security Handbook: A Guide for Managers sp800-100,* 2006, *http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf*

[19] OECD, *Guidelines for the Security of Information*, 2002, *www.oecd.org/dataoecd/16/22/15582260.pdf*

Recommendations include that organisations[5]:

- Manage security risk;
- Implement and maintain security policies;
- Establish security roles and responsibilities;
- Develop technical security; and
- Educate staff members.

While the approach to governance frameworks may vary from organisation to organisation due to differing needs, their definition subscribes to a core set of principles for information security. The techniques and frameworks discussed in the Governance paper provide a valuable mechanism for ensuring the Principles outlined herein are effectively adopted.

Principles of Information Security

While convergence has introduced new challenges to ensuring the security of information, the fundamental principles of information security have remained relatively consistent over the years despite this technological change. The Principles of Information Security presented in this report are:

1. *Information Security Is Integral to Enterprise Strategy*
2. *Information Security Impacts on the Entire Organisation*
3. *Enterprise Risk Management Defines Information Security Requirements*
4. *Information Security Accountabilities Should be Defined and Acknowledged*
5. *Information Security Must Consider Internal and External Stakeholders*
6. *Information Security Requires Understanding and Commitment*
7. *Information Security Requires Continual Improvement*

Figure 9 summarises the relationship between these principles, and Enterprise Architecture components in the convergence scenario. The Principles (outer ring) should be used to define and design the Enterprise Architecture (inner ring) in ensuring convergence within and across Enterprise Architecture components occurs in a secure manner.

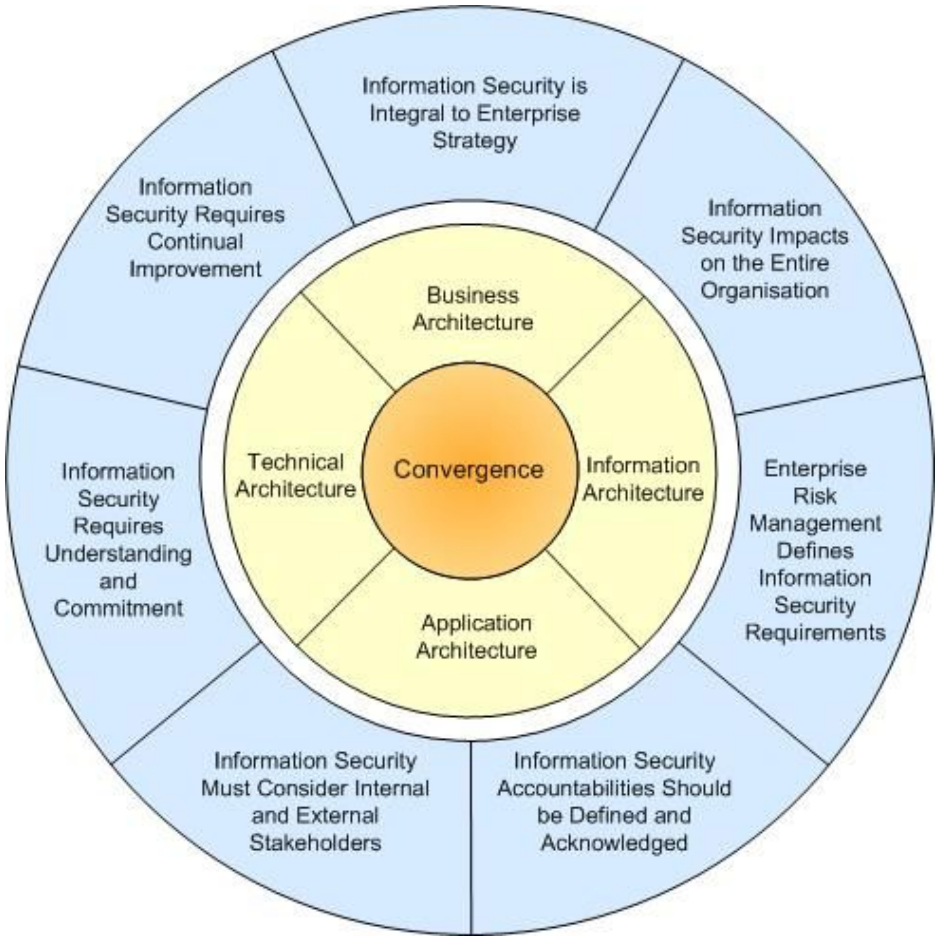


Figure 9: Relationship between Principles of Information Security, Enterprise Architecture and Convergence

A number of existing sets of information security principles were used in the development of the Principle set put forward in this report. These include:

- US National Institute of Standards and Technology (NIST)—Generally Accepted Principles and Practices for Securing Information Technology Systems (September 1996);
- OECD Guidelines for the Security of Information: Towards a Culture of Security (July 2002);
- Information Systems Security Association (ISSA)—Generally Accepted Information Security Principles (GAISP) (August 2003);
- ISO 27001—Information technology—Security techniques—Information security management systems—Requirements (June 2006); and
- Trusted Information Sharing Network (TISN)—Leading Practices and Guidelines for Enterprise Security Governance (July 2006).

NIST Generally Accepted Principles and Practices for Securing Information Technology Systems

The *Generally Accepted Principles and Practices for Security Information Technology Systems* report was published by NIST in September, 1996. The document seeks to provide a foundation for organisations to ensure security is maintained when conducting multi-organisational as well as internal business. The document offers eight principles and fourteen practices. The principles offer 'intrinsic expectations' which must be met when securing IT systems. The practices are the next level, where they provide a 'foundation for common IT security practices that are in general use today'. Practices can either map to one or more principles; in some cases they are constrained by principles[20].

While some principles and practices are applicable to the entirety of the information security discipline, they are specifically developed as guidelines for the management of computer systems. This report preceded world events such as increased focus on corporate governance at the turn of the century and the changing threat of terrorism demanding a more whole-of-enterprise approach to security. Given these changes in the environment, there was a necessity to update this list of principles for today's audience.

OECD Guidelines for the Security of Information

The *Guidelines for the Security of Information: Towards a Culture of Security* report was published by OECD in July, 2002. The guidelines are a direct response to the changing security environment by promoting the development of a 'culture of security'[19]. The document consists of nine information security principles which apply at policy and operational levels to assist participant nations in developing a culture of security. As this document is specifically applicable at a governmental level, appropriation of these principles to an organisational context was required.

ISSA Generally Accepted Information Security Principles

The *Generally Accepted Information Security Principles* is the successor of the Generally Accepted System Security Principles (GASSP) developed by the International Information Security Foundation (IISF). The document is developed with the aim of establishing guidance to standardised information security practice similar to the manner in which the Generally Accepted Accounting Practices (GAAP) are applied to the accounting profession.

The principles are developed in line with the OECD Guidelines for the Security of Information, and contain three levels of information security principles. These are[21]:

- Pervasive principles—rarely changing, fundamental principles targeting a governance level audience (including Boards and CEOs);
- Broad functional principles—changing only when reflecting major developments in technology or other affecting issues targeting operational management; and

[20] The United States National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 1996, *http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf*

[21] Information Systems Security Association, *Generally Accepted Information Security Principles*, 2003

- Detailed principles—numerous, specific and change frequently as technology and other affecting issues evolve with an information security practitioner audience.

The final version (3.0) of this document is dated August 2003 with the detailed principles yet to be completed. The set of pervasive principles provided in this document provides a foundation for considering information security implementation at an enterprise strategy level. However the development of closer ties between the information security principles and organisational strategy was considered necessary.

ISO 27001

ISO/IEC 27001—Information technology—Security techniques—Information security management systems—Requirements, commonly known as ISO 27001 is the international information security management system (ISMS) standard. The standard is preceded by AS/NZS 7799.2 and BS 7799.2.

The standard indicates that the adoption of an ISMS should be a 'strategic decision' for an organisation. "The design and implementation of an organisation's ISMS is influenced by their needs and objectives, security requirements, the processes employed and the size and structure of the organisation. These and their supporting systems are expected to change over time. It is expected that an ISMS implementation will be scaled in accordance with the needs of the organisation."[22]

The standard provides practical recommendations for the implementation of an ISMS rather than discrete principle level statements. However, the perpetual alignment with the organisation's business objectives concept is a key intrinsic concept for enterprise information security.

Information Security Management System (ISMS)

An ISMS is a component of the overall organisational management system. This component uses a business risk approach, in order to establish, implement, monitor, review and maintain controls in order to improve information security.

The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Source: Adapted from ISO 2700122

TISN Leading Practices and Guidelines for Enterprise Security Governance

The TISN *Leading Practices and Guidelines for Enterprise Security Governance* report provides eleven core principles documenting leading practice for security governance. These principles serve as a primary driver for defining all security governance roles, responsibilities, functions and activities[5].

The principles developed in this paper map to the core principles of security governance and established practical recommendations of how they can be implemented. See Figure 7.

[22] ISO, *ISO/IEC 27001—Information Technology—Security Techniques—Information Security Management Systems—Requirements*, 2006, Standards Australia/Standards New Zealand

Mapping of Proposed Principles to Existing Approaches

This report contains seven information security principles which are the result of a consensus built on the existing sets of principles discussed above, tailored to the context of Enterprise Architecture.

Table 1 provides a mapping between existing principle sets previously outlined and the seven principles presented in this paper. The principles put forward in this paper are listed at the left of Table 1, and the table indicates by a tick where this principle is also covered by the relevant previous principle set. Where not marked, the principle is not specifically included in the previous principle set.

An additional mapping against individual documents is provided in Appendix B.

Principles of Information Security	**NIST**	**OECD**	**ISSA GAISP**	**27001 ISMS**	**TISN Gov'**
1. Information Security is Integral to Enterprise Strategy	✓			✓	✓
2. Information Security Impacts on the Entire Organisation	✓	✓	✓	✓	✓
3. Enterprise Risk Management Defines Information Security Requirements	✓	✓	✓	✓	✓
4. Information Security Accountabilities Should be Defined and Acknowledged	✓	✓	✓	✓	✓
5. Information Security Must Consider Internal and External Stakeholders	✓	✓	✓		✓
6. Information Security Requires Understanding and Commitment		✓	✓	✓	✓
7. Information Security Requires Continual Improvement	✓	✓	✓	✓	✓

Table 1: Mapping of information security principles to existing knowledge base

Note: ISO 27001 ISMS mapping is adapted from ISO / IEC 27001-2006, Annex B Table B.1[22]

Relationship to Information Security Standards

The Principles of Information Security contained in this paper support achieving business strategy level justification and guidance for enterprise information security governance. By including the Principles of Information Security described in this document into the Enterprise Architecture, the organisation positions itself to satisfy the spirit of almost any regulatory framework for information security. The recommendations of each principle provide more practical examples of how the principles can be deployed within the organisation to enhance the 'culture of security' and achieve compliance requirements.

However, in order to holistically apply these information security principles, organisations should utilise information security standards in defining:

- The practical and technical application of information security controls; and
- The detailed process of security adoption.

Information security standards can assist organisations to:

- Set information security goals—benchmark the level of achievement for enterprise information security;
- Develop a roadmap to achieving the goals—assist in setting the strategic and operational planning in achieving the benchmarks set; and
- Validate the level of achievement—assess the level of compliance to the specified benchmark.

There are two types of information security standards, control based standards and maturity based standards.

Examples of Control based standards include:

- ISO 17799—Information technology—Security techniques—Code of practice for information security management; and
- ACSI 33—Australian Government Information and Communications Technology Security Manual, where relevant.

Examples of Maturity based standards include:

- ITIL—Information Technology Infrastructure Library;
- COBIT—Control Objectives for Information and Related Technology; and
- COSO—Committee of Sponsoring Organizations of the Treadway Commission Internal Control Framework.

The following section provides a brief description of each of these standards. An evaluation as to their ability to assist in implementing the principles set out on this document is also tabled for each. *Principle implementation* indicates where the standard can be used to apply the principle at a more granular and operational level within an organisation. *Principle measurement* indicates where the standard can be used to audit the application of the principle throughout the organisation's implementations.

ISO 17799

ISO/IEC 17799—Information technology—Security techniques—Code of practice for information security management commonly known as ISO 17799 provides best-practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining the organisation's ISMS. The standard offers controls within eleven domains of enterprise information security[5].

The scope of coverage is extensive, including controls for staff, review and compliance, physical security and strategic management elements. Thus, ISO 17799 can be used to develop and select appropriate controls with which to implement the principles of information security and consequently to validate the level of achievement.

ISO 17799	Principles of Information Security						
	1	2	3	4	5	6	7
Principle implementation	✓	✓	✓	✓	✓	✓	✓
Principle measurement	✓	✓	✓	✓	✓	✓	✓

Table 2: Mapping of Principles to ISO 17799

ACSI 33

The 'Australian Government Information and Communications Technology (ICT) Security Manual' (also known as ACSI 33) is developed by the Defence Signals Directorate (DSD) to provide policies and guidance to Australian Government agencies on how to protect their ICT systems.[23] ACSI 33 contains nine directives on security administration and ten standards of practice.

ACSI 33 drills down to a significant level of detail in terms of the specific configurations expected of government agencies. Although intended for a government audience, ACSI 33 controls can be used as a point of guidance by any organisation, and can assist in providing guidance on control types that may be suitable to achieve a level of protection.

ACSI 33	Principles of Information Security						
	1	2	3	4	5	6	7
Principle implementation		✓	✓	✓	✓	✓	✓
Principle measurement		✓	✓	✓	✓	✓	✓

Table 3: Mapping of Principles to ACSI 33

ITIL

The *Information Technology Infrastructure Library* is a customisable framework of best practices that promote quality computing services in the information technology (IT) sector. ITIL was originally created by a UK government agency Central Computer and

[23] Defence Signals Directorate, *ACSI 33 Australian Government Information and Communications Technology Security Manual*, 2006, *www.dsd.gov.au/library/infosec/acsi33.html*

Telecommunications Agency (CCTA) and is now adopted and used worldwide as a standard for best practice in provisioning IT Services.[24]

A component of ITIL—ITIL Security Management, based on ISO 17799—is of particular relevance to the application of the information security principles. The ITIL Security Management component is procedure based and includes ITIL standard processes such as service level, incident and change management processes. A key concept is that security should be perceived as a service and be incorporated into Service Level Agreements (SLAs).

ITIL	Principles of Information Security						
	1	2	3	4	5	6	7
Principle implementation		✓	✓	✓	✓	✓	✓
Principle measurement		✓	✓	✓	✓		✓

Table 4: Mapping of Principles to ITIL

COBIT

The 'Control Objectives for Information and related Technology' is a set of best practices for IT governance created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. The COBIT framework contains thirty-four IT processes in four domains—Planning and Organisation, Acquisition and Implementation, Delivery and Support, and Monitoring. These IT processes provide a basis for establishing and maintaining good security.

Of particular relevance to the implementation of the principles of information security, these COBIT IT practices can be used to define the information security tasks. Furthermore, the 215 specific Control Objectives which elaborate upon the IT practices provide business relevance as to why information security is required at a strategic level[25]. The Implementation Tool Set, Management and Audit Guideline documents can be used to implement and validate these detailed controls.

COBIT	Principles of Information Security						
	1	2	3	4	5	6	7
Principle implementation	✓	✓	✓	✓	✓	✓	✓
Principle measurement	✓	✓	✓	✓	✓	✓	✓

Table 5: Mapping of Principles to COBIT

[24] ITIL & IT Service Management Zone, *What is ITIL*, 2002, *www.itil.org.uk/what.htm*

[25] IT Governance Institute, *COBIT(3rd Edition) Executive Summary*, 2000, Information Systems Audit and Control Foundation

COSO

The US Committee of Sponsoring Organizations (COSO) of the Treadway Commission published an internal control framework in 1994 which subsequently served as a basis for standards such as COBIT. Key concepts developed in this framework are prevalent in a number of contemporary risk management and corporate governance approaches.

COSO requires that a formal risk assessment be performed to evaluate the internal and external factors that impact an organisation's performance. The results of the risk assessment will determine the controls that need to be implemented. COSO focuses on financial controls but also has implications for functions like information security.

COSO	**Principles of Information Security**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Principle implementation	✓	✓	✓		✓		✓
Principle measurement	✓	✓	✓		✓		✓

Table 6: Mapping of Principles to COSO

Principles of Information Security

1. Information Security Is Integral to Enterprise Strategy

Information security is a key support to the business objectives of enterprise strategy by both minimising risk and enabling trust to be maintained in new generations of services. Given this, information security must have the endorsement and support of executive management and the Board.

Mission vs. Strategy

The Mission describes the long term goals of the organisation. It embodies the purpose or broader goal for the organisation being in business. It serves as an ongoing guide without time frame.

The Strategy meanwhile outlines the progressive direction the organisation intends to take in order to achieve the mission. Strategic objectives provide a shorter-term guide for planning.

Source: Adapted from Cochran[26]

The effective deployment of information security controls compliments the enterprise mission by both:

- Protecting physical and financial resources, reputation, legal position, employees and other tangible and intangible assets; and
- Providing opportunities to introduce new services and connect to business partners with confidence.

To effectively support enterprise strategy, information security requires the support of executive management and the board.

Recommendation 1.1: Develop information security strategy consistent with the business goals and overall responsibilities of the organisation, with Board-level approval

The purpose of information security governance is to limit the risk of information compromise in order to more effectively enable an organisation to pursue its business goals. However, security is often perceived as an impediment to the operational requirements of the business. In order to achieve a 'culture of security'[19] within an organisation, information security must be clearly shown to be assisting in the pursuit of the organisation's mission.

In order to demonstrate this and position security effectively, organisations should:

- Determine the business objective of security by considering the interest of stakeholders *[R5.1 ~ 5.4]*;
- Document an information security strategy, providing a clear statement on how information security in the organisation supports the enterprise's mission;

[26] C Cochran, *'Using Quality Objectives to Drive Strategic Performance Improvement', Quality Digest Magazine*, 2000

- Implement an information security governance program to achieve the information security strategy of the organisation[5];
- Enhance the acceptance of information security through training and awareness programs *[R6.2]*;
- Engage operational executives in calculating the cost of information security incidents, and prioritising / approving information security investments in response; and
- Account for and protect all organisational intellectual property.

Case Study: Finance Services Organisation—Information Security Improvement

Scenario Context

An Australian finance services organisation underwent an information security improvement programme in 2006. The organisation undertook an initial gap analysis in mid-2005 where key business and security gaps were identified.

Key drivers for undertaking the program included:

- An industry regulator having expressed concern with regard to non-compliance to specific security related obligations; and
- Institutional customers of the organisation enquiring about the security of internal systems.

The organisation engaged external consultants to assist in the development and actioning of the programme which addressed these business drivers. Activities conducted include:

- Technical system reviews—including network security, application security, operational security processes, and access control
- Security policy framework review and redevelopment;
- Introduction of a Security Management Committee including representatives from key technology and business teams within the organisation; and
- Development and deployment of an organisation wide information security awareness program

Developments

The program brought a number of business benefits to the organisation including:

- Achieving regulatory acceptance of the security programme and resolution of outstanding regulatory audit items;
- Achieving faster deployment of products into institutional clients through addressing security considerations up front;
- Formalised processes to ensure future systems development and implementation in corporate security from the outset, avoiding the excess cost

of retrofitting security; and

- More educated and informed staff and the development of a culture of security to support the more rapid identification of security issues or incidents.

Lessons Learnt

- Information security initiatives must assist the organisation in addressing the business goals of the organisation *[R1.1]*;
- Incorporating security into the business process at the initial stages of development reduces overall cost to business. *[R2.5]*;
- The risk assessment process drives information security by identifying key business and security gaps. *[R3.1]*;
- A key driver for security for organisation is the requirement by customers – whether they are individuals or institutions. *[R5.2]*; and
- Revision and redevelopment of security policies and establishment of an effective employee awareness program are critical to the information security improvement programme. *[R6.1 and 6.3]*.

Case Study 1: Finance Services Organisation—Information Security Improvement

Recommendation 1.2: Ensure consistency of information security planning with strategic and operational planning

Information security, in supporting the business goals, aids an organisation's ability to provide services to customers and make profit. An organisation's information security initiatives should be subject to the same process of strategic and operational planning as is used for other enterprise business units. This planning process should be mandatory within the information security governance framework.

Long term planning should support an organisation's mission and long term strategy. To achieve this, organisations should:

- Maintain and increase profit by managing information security risks and minimising loss arising from security incidents;
- Maintain brand value by meeting industry security benchmarks and expectations and avoiding publicly disclosed security incidents; and
- Protect competitive advantage, proprietary knowledge and critical systems.

Short term planning should support an organisation's objectives and short term strategy. To achieve this, organisations should:

- Ensure current projects are deployed with appropriate security controls in place *[R2.5]*; and
- Implement controls to reduce identified vulnerabilities to an acceptable level of risk *[R3.2]*.

Recommendation 1.3: Executive management should demonstrate support for enterprise information security at all levels of the organisation

Leadership of the organisation should demonstrably support the effective implementation of information security controls. Executive managers should encourage support from throughout the organisation's hierarchy. Senior managers should understand the relevance and applicability of information security to their part of the business, and following from this understanding should seek to embed security into their business operations. Executive support is essential to instilling a 'culture of security' within the organisation.

Approaches to demonstrating management support throughout the organisation include:

- Executive management accepting ultimate responsibility for the state of enterprise information security, and allocating resources to information security programmes *[R4.1]*;
- Project managers incorporating security into the project development process, from project conception onwards throughout the project lifecycle *[R2.5]*; and
- Executive management ensuring their own compliance to information security policies and standards to demonstrate their commitment *[R4.3]*.

Recommendation 1.4: Ensure information security complies with legal and regulatory requirements

Australian critical infrastructure organisations are directly subject to a range of legal and regulatory requirements. This includes corporation, data protection and privacy laws *[R5.2]* and legislation such as Sarbanes-Oxley[27] abroad. Furthermore, industry specific legal and regulatory requirements exist for banking and finance, health, telecommunications, and many other industries. In many cases, it is necessary for enterprise information security to assist the organisation's corporate governance initiatives by ensuring compliance risk is addressed via information security controls.

In order to ensure compliance with legal and regulatory obligations, the information security team should:

- Support the Legal, Audit or Risk department (as applicable) in determining appropriate information security requirements for the organisation to meet compliance obligations;
- Develop information security metrics that provide validation of performance relevant to the compliance obligations; and
- Ensure procurement and contracting processes include consideration of the information security compliance obligations of the organisation and the comparative satisfaction of these by considered suppliers, systems and products.

Case Study: University of California, Berkeley – Legal and Regulatory Compliance

Scenario Context

On 11 March 2005, a computer from the offices of the Graduate Division of the

[27]United States of America, *Sarbanes Oxley Act of 2002*, 2007, *http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf*

University of California, Berkeley was stolen. The files on the laptop contained names, dates of birth, addresses and Social Security Numbers of 98,369 graduate students or graduate-school applicants. The files went back three decades in some cases.

Developments

The University notified all of the individuals affected by the data loss, as required by California State Bill (SB) 1386. SB 1386 went into effect on 1 July 2003, dictating that parties must disclose any breach of the security of personal data to any resident of California whose unencrypted personal information was, or was reasonably believed to have been, acquired by an unauthorised person.

As some of the compromised files went back to 1976, it was stated that school officials would have difficulty tracking down some of the people affected. The school created a special website to help individuals who found themselves suddenly vulnerable and also to help in contacting individuals for whom details were no longer available.

The university had previously recognised the legal requirement of SB 1386 and had amended their security policy. On April 29th, 2003 the University of California Office of the President issued an amendment to the university's *Business and Finance Bulletin IS-3—Electronic Information Security* to address these new legal requirements.

No incidents of identity theft have been reported related to the incident. However, the university did urge affected individuals to consider putting a fraud alert out at credit reporting agencies.

Lessons Learnt

- The impact of legal and regulatory change should be considered in revision cycles of security strategy and policy *[R1.4]*;
- Physical security is a key element of information security, and risks associated with physical compromise must be addressed in order to ensure appropriate risk mitigation. *[R2.3]*; and
- Organisations should develop an information security feedback process to incorporate incident details into future risk assessments. *[R7.4]*.

Further Information

http://itpolicy.berkeley.edu/protected.data.html

http://news.com.com/Laptop+theft+puts+data+of+98%2C000+at+risk/2100-1029_3-5645362.html

http://idalert.berkeley.edu/

Case Study 2: University of California, Berkeley—Legal and Regulatory Compliance

2. Information Security Impacts on the Entire Organisation

A holistic approach to implementing enterprise information security is the most cost-effective. This involves considering people, technology and processes throughout all areas of the business. To maximise return on security investment, information security must be designed into information systems and processes from the outset.

Return on Security Investment

Return on Security Investment is the benefit to the organisation as a result of spending on security initiatives. It relies on the simple yet powerful concept of *Return on Investment* - 'Which of these options gives me the most value for my money?'

Return on Security Investment can be used to:

- Compare alternative security investment strategies; and
- Justify security investment.
- Source: Adapted from Sonnenreich et al.[28]

A holistic approach ensures that information security achieves:

- Whole-of-organisation acceptance and cooperation;
- Information security implementations that are practical, well integrated and address business needs; and
- The cost-effective inclusion of appropriate security controls.

Recommendation 2.1: Include representatives of all areas of the organisation in information security decision making

Information security risks and their corresponding controls will often touch all areas of an organisation. Security weaknesses – whether technical or procedural – in one area of an organisation can increase the information security risk across the enterprise. Additionally, information security controls implemented without consideration for the impact on the full range of business areas within the organisation may prove to be clumsy, inefficient or could adversely impact the organisation's core business.

Consequently, it is in an organisation's best interests to ensure that strategic business units throughout the entire organisation actively participate in information security initiatives. Where an organisation is comprised of multiple entities (whether foreign divisions or subsidiary companies), an overarching view of the information security requirements should be established. This heightened degree of cooperation and coordination of information security between enterprise divisions supports the effective development of a 'culture of security'.

[28] W Sonnenreich, J Albanese, & B Stout, '*Return on Security Investment (ROSI): A Practical Quantitative Model', Journal of Research and Practice in Information Technology, vol. 38, no. 1,* 2005, *http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT38/JRPIT38.1.45.pdf*

By incorporating representatives from across the organisational structure, the organisation:

- Achieves whole-of-organisation buy-in to information security;
- Ensures the practicality of information security solutions;
- Addresses the interdependency of Enterprise Architectures; and
- Provides an avenue for cooperative dialogue on information security.

To achieve this, organisations can:

- Implement an information security steering committee, comprising of representatives of key stakeholder groups and reporting to the CEO, board audit committee and the risk management committee (if in place);
- Conduct periodic internal workshops involving stakeholders in information security across the organisation; and
- Require business units to state compliance to information security policies periodically.

Recommendation 2.2: Implement enterprise processes that support practical and timely solutions for information security

In the event that material information security risks exist within an organisation, that organisation should focus on practical and timely solutions for information security rather than the process of formalising standards. Where the documentation and approval process delays the practical deployment of security, it is in the best interests of an organisation to provide exceptions for stop-gap security practices in the interim.

In order to support practical and timely solutions, the information security team should:

- Request business stakeholders provide an assessment of the impact of proposed information security standards, procedures and guidelines prior to their approval;
- Provide clear and understandable information security communications by using terms and language suitable for the audience *[R6.1 and 6.3]*;
- Provide emergency change request and exception handling processes for stop-gap fixes where required;
- Consider tested, proven and reliable information security solutions first *[R2.6]*;
- Define efficient escalation channels to obtain expeditious approval for changes and exceptions;
- Assign accountability to interim fixes and responsibility for providing a formal solution *[R4.3]*; and
- Exercise and train staff on their responsibilities to ensure they can communicate and respond to information security issues as efficiently as possible *[R6.2]*.

Recommendation 2.3: Consider physical security aspects of information protection within ‘information security’

Information security governance requires the protection of information in all its forms, including the protection of hard copy records and appropriate processes for personnel selection.

Similarly, IT processing facilities require both logical and physical protection to prevent damage or theft.

Inconsistency between the management of physical security and information security can introduce additional risks to an organisation. Conversely, through information sharing and cooperation, physical security personnel can provide information security personnel with the ability to more effectively detect and respond to a range of security incidents.

To align information and physical security, organisations can:

- Define the organisation's security strategy to govern both Information Technology (IT) and physical aspects of information security;
- Assign both physical and information security responsibilities to security officers *[R6.3]*; and
- Subject change requests to comprehensive reviews which include both physical and information security elements.

Recommendation 2.4: Engage the human resources department to ensure people are managed as a component of information security within the organisation

The development of an effective 'culture of security' within an organisation is directly dependent on its people. Personnel security must be managed for information security to be effective. As employees are fundamental to any organisation, the human resources function must support information security in ensuring employee knowledge and behaviour reduces information security risk.

Human resources can assist with the establishment of effective personnel security processes throughout the employment lifecycle, through:

- Evaluating the suitability of the prospective employee from a security perspective by conducting adequate background checks;
- Including security training in the induction process. Where authorisation and access provisioning to physical and information assets are required, these should be conducted in a uniform manner *[R6.2]*;
- Maintaining the level of personnel related information security risk at an accepted level on an ongoing basis. This may include incorporating information security into performance management, regular awareness programs and exercises. *[R7.3]*; and
- Assisting information security in the removal of access rights in a timely manner upon the dismissal or departure of an employee.

Case Study: Centrelink—Monitoring of Staff Access to Customer Records

Scenario Context

In August 2006, Centrelink announced the interim results from a strengthening of the system used for monitoring staff access to customer records. This monitoring system had been in place for 13 years, with Centrelink continuing to invest in

improving the analysis capabilities provided by the system over time.

Centrelink staff are subject to requirements under the Australian Public Service Code of Conduct and the Privacy Act to handle customer information appropriately, and it is specifically considered inappropriate for a staff member to access a customer record without a genuine business need. This includes access to the records of relatives or friends, even if it is at their request, where a genuine business purpose does not exist.

Centrelink staff members receive ongoing communication regarding their responsibilities when it comes to dealing with sensitive customer information, and the organisation's right to monitor such access. Training is also conducted to raise staff awareness of issues such as ethics, privacy and fraud.

Furthermore, Centrelink's Privacy Awareness Kit, includes a 'conflict of interest' and 'browsing' policy, that is available to all employees via the Centrelink intranet, and sets clear requirements for staff behaviour and penalties for policy breaches.

Developments

Over the course of the year, Centrelink identified inappropriate access to customer records by a number of staff, which led to the dismissal of 19 members of staff, 92 resignations, more than 300 staff facing salary deductions and fines, and a further 46 reprimands with others demoted or issued a warning. There were a total of 585 staff sanctioned through this process.

Centrelink CEO Jeff Whalan stated that this result demonstrated the action being taken to ensure privacy and integrity of social security data, but pointed out that of the agency's 25,000 staff, only 2 percent had behaved inappropriately.

Lessons Learnt

- Organisations need to observe legal responsibility (in this case matched by the Australian Public Service Code of Conduct, privacy and confidentiality policy level requirements), and ensure these requirements are matched by organisational policies. *[R1.4]*;
- Employee education programs must be coupled with effective monitoring practices to assess the degree of compliance to the stated goals. *[R6.2]*;
- Support for security from executive management is essential to effective implementation. *[R1.3]*; and
- Human Resources can assist in the education and monitoring of staff usage activity *[R2.3 and 7.3]*.

Further Information

http://www.centrelink.gov.au/internet/internet.nsf/news_room/06nat_privacy_protection.htm

Case Study 3: Centrelink—Monitoring of Staff

Recommendation 2.5: Embed information security within the lifecycle of enterprise information systems

The organisation's information security governance framework should establish processes and define responsibilities to allow security to be considered at the outset of information systems development. Considering security during the conception stage drastically reduces the cost of security throughout the system's lifetime (see Figure 10). Initial considerations at the conception stage allow security to be embedded within the lifecycle of the system. Organisations should recognise that different IT systems have varying security requirements. Such system-specific requirements must be considered in the selection of an IT solution and incorporated into system design.

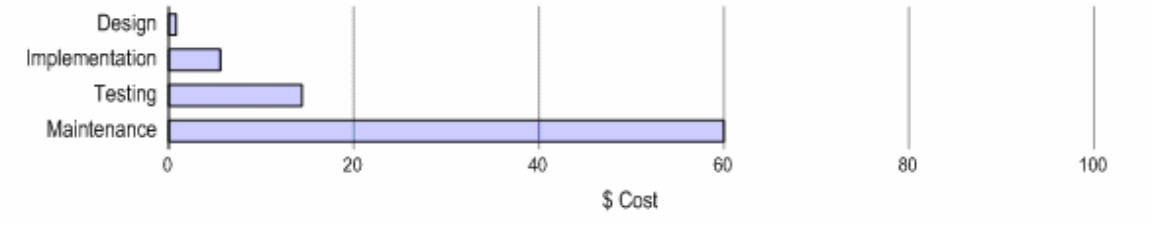


Figure 10: Remediation Cost Multiplier by System Lifecycle Phase[29]

For security to be most effective throughout the lifecycle of information systems, organisations should:

- Document and communicate assumptions and design decisions that may impact on the security of a system;
- Include a "security requirements specification" as a partner document to functional requirements;
- Execute rigorous security testing of systems prior to production deployment;
- Implement exception procedures for non-compliant components (including a timeline and path for resolution) *[R3.2]*;
- Request and evaluate evidence of product security from vendors when considering implementing proprietary solutions *[R7.5]*;
- Maintain security of information throughout the information lifecycle (i.e. creation, processing, storage, deletion and destruction);
- Develop and maintain a periodic assurance audit and testing plan; and
- Execute destruction and decommissioning of computer media in line with best practices such that no sensitive information remains.

[29] @Stake 2002 as cited in J Reavis, *"CSO White Paper Series - Managing Risk and Reducing the Cost of Web Application Security", CSO Informer,* SPI Dynamics, 2004, *http://www.securitytechnet.com/resource/security/application/SPI-risk-cost-draft-ver2.0.pdf*

Case Study: Aged-Care Facility—Access Control Design

Scenario Context

An aged-care facility in rural New South Wales offering single room accommodation for approximately 30 residents began the adoption of an electronic record keeping facility to replace the current paper record keeping system. Information stored included personal, financial and medication information about each resident and contact details for the staff and visiting professionals.

The proposed electronic version of the system was intended to provide:

- Intranet access to the health information stored on a server system;
- One PC to be used by the administration manager;
- A number of PCs made available for use by the health care staff; and
- Mobile devices to be used by doctors and physiotherapists which connect into the network dynamically.

Developments

The aim of defining access control restrictions for the various roles in the organisation was to maintain, at minimum, the confidentiality level of the current paper-based system and, ideally, to achieve a strict need-to-know access scheme. To support this, a clear summary of user access/authorisation levels was provided prior to design, and included:

- **Managers**—broadest access to the information, however not unrestricted access. Managers can insert past medical records when residents are admitted, though they cannot subsequently add medical entries. Also, managers cannot view the private notes of doctors and cannot sign legal agreements on behalf of a resident;
- **Health Care Workers—**required signing a confidentiality agreement before they have access to any resident data. Their main form of access is to view the care plan for each resident and to add progress note entries based on their observations; and
- **Residents**—privacy laws require that a person have full access to any information stored about them (unless the well-being of a third party would be jeopardised by revealing the information).

Lessons Learnt

- By considering security at the outset during the design phase, the aged-care facility generated a higher return on investment and reduced overall security cost. *[R2.5]*;
- In the implementation of access controls for a new system, the level of access must match the business purpose and system use scenario. *[R4.3]*;
- Through access controls, the aged-care facility seeks to ensure sensitive customer and community data is protected appropriately. *[R5.2]*; and

- As elderly residents are to be granted access to their personal information, awareness training and education of IT and security for residents is required. *[R6.2]*.

Further Information:

http://crpit.com/confpapers/CRPITV32Evered.pdf

Case Study 4: Aged-Care Facility—Access Control Design

Recommendation 2.6: Implement security based on transparent, trusted and proven solutions

Security solution selection should be based on a practical decision of environmental fit, operational appropriateness and cost-benefit. However, as a general rule, organisations should consider solutions which have been proven, tested and independently verified.

Security Through Obscurity

Security through obscurity refers to an attempt to use secrecy (of design, implementation, etc.) to ensure security.

A system relying on security through obscurity may have theoretical or actual security vulnerabilities, but its owners or designers believe that the flaws are not known, and that attackers are unlikely to find them. This technique stands in contrast with *security by design*, although many real-world projects include elements of both strategies.

Source: Adapted from S/Keysource.com[30]

Proven solutions provide the organisation with a greater level of assurance as they have generally been subject to rigorous scrutiny by other implementers in the marketplace. The product may also have been assessed to a certain "Assurance Level" under a program such as the Common Criteria[31].

Security solutions that are poorly documented, or have not been widely reviewed or tested, are more likely to be subject to risks associated with "security through obscurity".

Furthermore, proven solutions are likely to be easier to implement, manage and review as there is more information available about the supporting processes and procedures and a greater accessibility of qualified/trained personnel.

[30] S/Keysource.com, *Security Through Obscurity*, 2007, *http://www.skeysource.com/one-time-password/security-through-obscurity.html*

[31] Common Criteria Portal, 2007, *http://www.commoncriteriaportal.org/*

Common Criteria

Common Criteria is an international standard (ISO 15408) for computer security. As the name suggests, it provides a common set of requirements for the security functionality of IT products, as well as assurance measures applied to these products during security evaluation.

The Common Criteria permits comparability between independent security assessment of hardware, firmware or software.

Source: Common Criteria Portal[31]

Some open and trusted information security initiatives which the organisation should consider include:

- Information security management standards such as:
  - ISO 17799 Information technology—Security techniques—Code of practice for information security management; and
  - Payment Card Industry Data Security Standard (PCI DSS).
- Best practice information system development and management processes such as:
  - Information Technology Infrastructure Library (ITIL)—a framework for best-practice approaches to delivering high quality information technology services. ITIL outlines an extensive set of management procedures which are supplier independent and provide the breath across IT infrastructure, development and operations;
  - Open Web Application Security Project (OWASP)—an open-source project dedicated to finding and fighting the causes of insecure software. The OWASP Guide provides methodology and processes for; and
  - Center for Internet Security (CIS)—a non-profit entity which seeks to reduce technical risk of business and e-commerce disruptions. CIS Benchmarks provide a standard level security configuration for information technology systems.
- Open encryption algorithms such as the Advanced Encryption Standards (AES).

Defence in Depth

Defence in Depth is the intelligent application of techniques and technologies, to achieve a balance between the protection capability and cost, performance, and operational considerations.

Source: National Security Agency[32]

Recommendation 2.7: Implement layered security

Organisations should recognise the need to provide coordinated and multi-layered security architectures to mitigate information security risks. In turn, security should not rely solely on point solutions as a single control failure may result in a complete compromise.

---

[32] The United States National Security Agency, *Defense in Depth*, 2007, *http://www.nsa.gov/snac/support/defenseindepth.pdf*

The US National Security Agency (NSA) has devised an approach entitled “defence in depth”. This approach requires a "layered" approach to security, such that the failure of a single control point will not result in a full system compromise. Additionally, the approach requires mechanisms to protect against attack, and also to detect such attacks, and provide an effective response.

In pursuing a layered approach to security, organisations should:

- Coordinate and ensure alignment of physical, personnel and IT security programs;
- Enforce separation of duties;
- Implement technical, procedural and operational controls;
- Develop and implement redundancy and contingency plans as part of the business continuity program; and
- Assess the impact and risk of control failure and ensure secondary controls are in place to address such an event.

3. Enterprise Risk Management Defines Information Security Requirements

A fundamental requirement of all business operations is the management of risk. As one component of this, organisations need to assess, protect against and report on information security risk.

The proposed treatment of risk, via introduction of information security requirements, must be proportional to the business impact of the risk.

Risk Management

*Risk Managemen*t is concerned with the possible reduction in business value from any source. Risk management is the activity which seeks to understand these risks and subsequently accept, mitigate, eliminate or transfer them.

Source: Harrington and Niehaus[33]

Driving information security risk management from the enterprise risk management function allows:

- The information security function to be aware of the business impact of information security;
- The information security function to be aware of risk management regulatory requirements;
- Enterprise risk management to be aware of technical controls in the management of information security risk;

[33] SE Harrington & GR Niehaus, *Risk Management and Insurance*, McGraw Hill – Irwin, 2004

- Information security risk treatment and prioritisation to be adapted to the business requirement of the organisation more effectively; and
- Justification of information security spending and mitigation of possible overspending.

Recommendation 3.1: Conduct information security risk assessments in line with the enterprise risk assessment methodology

In order to align corporate governance and information security governance, the enterprise risk management function should define the risk management methodology to be used in assessing and managing information security risk. Whether the methodology used is in accordance with a recognised standard or a custom developed methodology, the uniformity of the process provides an organisation's business leaders with a level of consistency in the rating and reporting of risks. In line with enterprise risk management, the scope of risk considered at the initial stage of the risk assessment should be as comprehensive as possible.

Reporting on the state of risk controls should be in line with the requirements outlined by enterprise risk management. This is to provide a level of consistency for executive management reporting and compliance purposes.

To ensure consistency in use of the enterprise risk assessment methodology within information security, the organisation should:

- Develop generic risk assessment guidelines to assist information security in developing a risk assessment methodology specific to information systems;
- Assess and approve an information security risk management methodology consistent with the enterprise risk management methodology;
- Review completed information security risk assessments outside of the information security department (e.g. Group Audit or Group Risk) to assess rating consistency between domains; and
- Use a schedule for assessment and reporting on information security in line with enterprise risk management standards.

Recommendation 3.2: Prioritise the treatment of risks and ensure the treatment is proportionate to the business impact

Risk management should ensure information security prioritises risk treatment solutions and strategies in terms of the business impact of associated risks. Furthermore, the treatment should be proportionate to the business value of the information system and the degree of reliance afforded, as well as the severity, probability and extent of potential harm.

In order to appropriately treat risks, personnel with risk management responsibility should assist the information security team in developing:

- an asset and risk register of all information security assets and risks;
- a method for materially comparing risks and their treatments via cost / benefit analysis; and
- developing a risk schedule and assigning priorities to risks.

To complement this, the information security team should:

- Develop a risk schedule and resolution plan which is incorporated into enterprise level risk tracking by the enterprise risk management team; and
- Monitor the performance of risk mitigation activities to ensure these remain appropriate and proportionate to the business impact.

Case Study: Yarra Valley Water—AS 7799.2 Certification

Scenario Context

The Management and Board of Yarra Valley Water (YVW) recognised that certifying its Information Security Management System (ISMS) would provide benefits in improved efficiency, higher quality of service and increased value to the organisation.

Executive approval of the IT Security Strategy was given in August 2002 with a goal for certification being achieved in the first half of 2004. The process involved many key milestones and culminated in SAI Global conducting the final certification audit in May 2004, which formally passed YVW for compliance to the standard.

The key to YVW's success was being able to leverage from and re-use the processes, policies and products from YVW's experience in standards in other areas of operations. These included ISO 9000, ISO 14000 and Hazard Analysis and Critical Control Points (HACCP), AS 4360, ISO 4301 and the IT Infrastructure Library (ITIL).

Developments

The ISMS has now ensured that security is absorbed into YVW culture as evidenced by the continual compliance with the ISMS that is confirmed by surveillance audits and tri-annual recertification.

The attitudes, methodologies and procedures that are in place to achieve and maintain ISMS certification helps YVW realise a return on investment due to:

- Lower losses associated with security incidents through resilience against such events as malware threats;
- Improved customer and public perceptions of YVW as being a well managed organisation;
- Lowered public liability and professional indemnity insurance premiums—savings on premiums the first year alone resulted in payback of YVW ISMS expenditure in less than 9 months; and
- Increased efficiency of the Victorian Attorney General's Department annual review of IT at YVW.

Lessons Learnt

- Leverage existing processes into a whole of organisation security management

program, reducing the need for staff to re-learn processes and incur extra expenses. *[R2.2]*;

- Information security should seek to improve service continuity to customers *[R5.1]*; and
- Executive support and approval for the information security program is essential for its suitability to the organisation and long-term sustainability *[R1.1 and 1.3]*.

Further Information

www.sai-global.com/NEWSROOM/TGS/2005-02/YARRAVALLEY/YARRAVALLEY.HTM

www.sai-global.com/NEWSROOM/TGS/2004-07/WATER/WATER.HTM

http://www.dpc.vic.gov.au/domino/Web_Notes/newmedia.nsf/35504bc71d3adebcca256cfc0082c2b8/e241ea7d87820dd8ca25703f002805db!OpenDocument

www.cio.com.au/index.php/id;216935928;fp;4;fpid;21

www.standards.org.au/cat.asp?catid-64&contentid=28&News=1

Case Study 5: Yarra Valley Water—AS 7799.2 Certification

4. Information Security Accountabilities should be Defined and Acknowledged

Organisations should develop and formally implement information security responsibilities within the enterprise. These responsibilities exist internally and may also extend across organisational boundaries to outsourcers, business and service partners, or customers. All users of information systems should be informed of the consequences of their actions.

Accountability vs. Responsibility

Responsibility is a broad term defining obligation and expected behaviour. The term implies a proactive stance on the part of the responsible party and a causal relationship between the responsible party and a given outcome.

Accountability refers to the *ability to hold* people responsible for their actions. Therefore people could be responsible for their actions but not held accountable. A fiduciary duty exists in situations where this accountability is enforceable by law – such as a CEO's responsibility for good corporate governance.

Source: US National Institute of Standards and Technology[34]

The responsibilities and relationships between individuals, processes and information should be clearly defined, documented and acknowledged as per corporate governance requirements.

By defining and establishing information security responsibilities, the organisation:

- Enhances executive recognition and acceptance of their accountability for the state of enterprise information security;
- Institutionalises information security by embedding employee requirements within the employment contract and job descriptions; and
- Enhances employee awareness of information security threats, operations and controls.

Recommendation 4.1: Hold executive management accountable for the state of enterprise information security

Corporate governance reform has placed legal responsibility on officers of an organisation to discharge their duties with a degree of care and diligence[35]. Officers also have a responsibility to act in a manner which does not cause detriment to the corporation[36]. These requirements include the management of information security risks.

In order to manage the chief executive's accountability for information security to external stakeholders, internal accountability for information security should be formally allocated

---

[34] National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 1996, *http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf*

[35] Commonwealth of Australia, *Corporations Act 2001, section 180 subsection 1*, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html*

[36] Commonwealth of Australia, *Corporations Act 2001, section 182 subsection 1*, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s182.html*

through the use of key performance indicators. This will ensure that information security is given due consideration in all aspects of an organisation's activities.

A number of actions can assist executive management in meeting their information security responsibilities, including:

- Structuring enterprise information security to be in line with enterprise mission and strategy *[R1.1]*;
- Incorporating information security as a key risk management and internal control mechanism *[R3.1]*;
- Delegating information security responsibilities and introduce effective escalation and reporting mechanisms *[R3.2]*; and
- Incorporating information security metrics into the key performance indicators (KPIs) of executive management roles.

Recommendation 4.2: Assign information security responsibilities throughout the organisation

All employees of an organisation have a responsibility for information security in order to support security governance and support the 'culture of security'. The allocation of specific roles and responsibilities to personnel within the organisation should take into account the importance of confidentiality, integrity and availability to each area of the business.

In order for information security responsibilities to be effectively assigned throughout the organisation, a number of best-practice conventions can be employed including:

- Utilising the separation of duties principle and consider organisational reporting structures in order to provide additional checks and balances to deter and detect malicious activity*[R3.2]*;
- Assigning technical responsibility for information security to an organisation's IT department;
- Appointing human resources as a key stakeholder in the definition of employee responsibilities, education and awareness initiatives in the area of information security, as well as monitoring of employee behaviour *[R2.4]*;
- Appointing a security architect to the Enterprise Architecture team; and
- Ensuring that all staff are provided with the necessary tools, knowledge and experience to be able to meet the information security requirements expected of them *[R7.1]*.

Case Study: Siemens Canada—Security Responsibility Definition

Scenario Context

In the 1990s, German manufacturing, IT and services company Siemens recognised the need for the enterprise Chief Security Officer (CSO) role to reside outside of the enterprise IT domain. According to Harald Hoefler, Chief Information Officer (CIO) of Siemens Canada, Information Security has reported to the Chief Financial

Officer's (CFO) office ever since.

The Siemens CSO has two primary roles:

- Auditing systems for adequate security; and
- Implementing sufficient security controls following from such an audit.

Hoefler suggests that the CSO can do neither well without independence from the CIO.

Hoefler presents the scenario where if the security officer reported directly to the CIO, security problems will be fixed without bringing them to the attention of top executives.

Developments

Hoefler suggests that the ideal situation is to have all the top executives aware of the problems with security, which then facilitates a cooperative effort across the organisation in fixing them. Without the attention and oversight of other senior executives, the CSO cannot ensure that the necessary audit issues are adequately addressed by the CIO's department.

The necessary level of disclosure and cooperation required in order for security issues to be comprehensively resolved, can occur only when security reports to an executive with broad managerial responsibilities for the company as a whole, such as the Chief Executive Officer (CEO), CFO or Chief Operations Officer (COO).

Different divisions within Siemens handle the specific security role differently. However, increasingly they are combining information and traditional corporate security under a CSO role, who reports to the CFO.

Lessons Learnt

Establish effective accountability for information security through extensive consideration of the organisational and reporting structure. *[R3.2]*; and

Ensure security is brought to the attention of top level executives in order to garner their support for information security. *[R3.1]*.

Further Information

www.cio.com/archive/041504/homeland.html

Case Study 6: Siemens Canada—Security Responsibility Definition

Recommendation 4.3: Allocate responsibility for information security to match business roles

As information security responsibilities are defined throughout an organisation, a mechanism is required to formally assign these roles and responsibilities to employees. Consequently, information security responsibilities should form a component of the employment or engagement contract and the job description. Achievement of information security objectives should be recognised by an organisation's performance management system.

Furthermore, users of information systems should be provisioned for a level of use and access rights which are suitable for the job role. Separation of duties should be enforced to prevent fraud and error. This is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users[38].

Least Privilege

Least Privilege is the concept that every user of a system should operate using the least set of privileges necessary to complete the task allocated to them.

Source: Adapted from Saltzer and Schroeder[37]

Provisioning of these rights should therefore adhere to the least privilege principle. Users can then accept accountability for the usage of their information system identities.

In order to effectively enforce responsibilities for information security, the organisation should:

- Include assessment against information security objectives in performance reviews with corresponding recognition;
- Clearly document and enforce an acceptable usage and user responsibility policy *[R6.1]*;
- Make information on security issues available to users – including supporting information security at home; and
- Provide training and practical exercises to ensure employees and contractors have the necessary capability to handle information security within their job role *[R6.2]*.

[37] JH Saltzer & MD Schroeder, *'The Protection of Information in Computer Systems', The Fourth ACM Symposium on Operating System Principles*, 1973, *http://www.cs.virginia.edu/~evans/cs551/saltzer/*

[38] RA Botha & JHP Eloff, *'Separation of Duties for Access Control Enforcement in Workflow Environments', IBM Systems Journal, vol 40, no 3*, 2001, *http://www.research.ibm.com/journal/sj/403/botha.pdf*

Recommendation 4.4: Define information security responsibilities for external parties in the engagement contract

Many organisations now outsource 'non-core' business functions, often including IT services, to external companies. Given the access to sensitive data and systems that these external companies will often have, the agreement and formalisation of information security roles and responsibilities is crucial to manage the risk of such engagements[39].

Outsourcing

Outsourcing refers to an arrangement by which a task that would otherwise be done by staff internal to the organisation is transferred to an external entity specialising in the management of that operation.

The primary difference between an outsourcing and a vendor relationship is that outsourcing replaces the internal capability to conduct a business operation and a service provider provides a factor of production.

As a result outsourcing involves transferring or sharing management control of a business function. To enable these, this involves a degree of two-way information exchange, coordination and trust between the outsourcer and its client.

This higher degree of integration subjects the client organisation to increasing security risks when compared to a traditional vendor relationship.

See more on the management of security in outsourcing in the TISN report: 'Managing IT Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure'[39].

In addition to organisations placing information security requirements on outsourcing partners or other suppliers, it is now increasingly common for such requirements to be placed on organisations by their own customers.

Both in situations where the organisation outsources business functions (e.g. to contracts, business process outsourcers, or consultants), and in situations where the organisation is a service provider themselves, it is necessary for a Service Level Agreement (SLA) to provide clarity of information security roles and responsibilities. Such an SLA will often include terms to ensure:

- The level of security at external parties is equivalent to that of the organisation itself *[R5.3]*;
- An agreed set of security standards and policies is in place between the parties *[R5.3]*;
- The co-ordination of information security activities such as audits and incident response *[R3.1]*; and
- The allocation of costs associated with remedying information security deficiencies is agreed prior to their occurrence.

[39] Trusted Information Sharing Network (TISN), *Managing IT Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure*, 2007, http://www.tisn.gov.au

Case Study: Multinational Payment Card Provider—Supplier Security Requirement

Scenario Context

A multinational payment card provider outsourced their outbound telephone marketing requirements to a medium-sized communications service provider. This service required the payment card provider to deliver to the communications service provider a large volume of customer numbers, and corresponding personal and payment card details.

Given the sensitivity of the information being communicated and stored by the service provider, the payment card provider required the communications service provider to agree to abide by their global security policy. Additionally, the communications service provider was required to complete a "self-assessment" audit of security controls, and submitted the outcome of this to the payment card provider.

A number of security shortcomings were identified, including the lack of an information security strategy, policy or standards, as well as a large number of technical implementation concerns including the lack of data encryption.

Developments

The payment card provider requested that the communications service provider deliver a compliance strategy to bring their operations into line with the global security policy. A gap analysis and costing was completed by the communications service provider, and a range of initiatives were undertaken to seek to reach the required level of security for their client.

While reaching this security standard was costly for the communications service provider, it ensured that the payment card provider's customer data was protected at a level equivalent to that of the original organisation, throughout the business process of outbound telemarketing.

Lessons Learnt

- Incorporating security considerations at the initial stages of system design would have reduced costs significantly for the company *[R2.5]*;
- Information security must consider internal and external stakeholders. When engaging service providers, it is the obligation for the organisation seeking services to effectively validate the standard of information security arrangements within the service provider and to determine its appropriateness *[R5.3]*; and
- The security responsibility for external parties should be defined within the engagement contract *[R4.4]*.

Further Information

www.csoonline.com.au/index.php/id;1863721000;fp;4;fpid;14

Case Study 7: Multinational Payment Card Provider—Supplier Security Requirement

5. Information Security Must Consider Internal and External Stakeholders

As the interconnectedness of systems grows, the importance of the security of each node is increased. The legitimate interest of stakeholders—including customers, suppliers and other business partners—should be considered in information security decision making. Critical infrastructure has a responsibility to meet the security expectations of the community at large.

Stakeholders

The term 'stakeholders' refers to any person or group—including investors, employees, customers, suppliers and in some cases the community at large—who are impacted by a given decision. The competitiveness and ultimate success of an organisation requires the support and commitment of all key stakeholders.

Consequently, the interest of stakeholders must be protected in order to retain long-term cooperation.

Source: Adapted from the OECD[40]

By considering internal and external stakeholders, an organisation can ensure that it:

- Protects customer (including upstream end user) interests;
- Ensures consistency in data protection throughout the chain of suppliers involved in delivering a product or service; and
- Ensures the maintenance of trust between the organisation and the community at large.

Recommendation 5.1: Implement information security controls to support service continuity

The availability of critical infrastructure systems is of significant importance and relevance to direct customers and often to the community as a whole. In order to ensure a suitable level of service continuity is maintained, information security must support the organisation in achieving consistent availability. This availability will often require consideration of the security controls in place at all links of the organisation's value chain (Figure 11).

Figure 11: Typical value chain

To ensure service continuity, organisations should:

- Assess the criticality of information infrastructure to service continuity *[R1.1]*;

[40] OECD, *OECD Principles of Corporate Governance*, 2002, *http://www.oecd.org/dataoecd/32/18/31557724.pdf*

- Implement Service Level Agreements (SLAs) with key partners or suppliers *[R5.3]*;
- Develop and exercise an effective incident response procedure;
- Structure and implement enterprise business continuity management programmes;
- Exercise and test business continuity and disaster recovery plans with the aid of dependent and supplier organisations; and
- Ensure customers are aware of service outages and assist them in contingency planning.

Recommendation 5.2: Ensure sensitive customer and community data is protected appropriately

Many critical infrastructure services require the collection and maintenance of sensitive customer data for ongoing operations. Similarly, these services often also involve the creation or use of information sensitive to a community or industry[41].

Legal Requirements

Privacy Amendment (Private Sector) Act 2000 NPP4 Data Security

Organisations must take reasonable steps to:

- Protect the personal information from misuse and loss and from unauthorised access, modification or disclosure; and
- Destroy or permanently de-identify personal information if it is no longer needed.

Section 52 of the Trade Practices Act 1974

Representations made by you or your employees regarding e-security must not be misleading or deceptive

ASX Listing Rule 3.1

Continuous disclosure to shareholders of price-sensitive incidents (which could include security breaches of customer information)

Corporations Act 2001

Company directors must take reasonable steps to be informed about issues which impact upon the company

Sources: Austlii[42,43], The Office of the Privacy Commissioner[44], Australian Securities Exchange[45]

[41] Trusted Information Sharing Network, *Infrastructure Information in the Public Domain,* 2006, *http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~infrastructure-information+in+the+public+domain.23-11-06.pdf/$file/infrastructure-information+in+the+public+domain.23-11-06.pdf*

[42] Commonwealth of Australia, *Trade Practices Act 1974, section 52,* 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/tpa1974149/s52.html*

Good governance dictates that the protection of such data is necessary to ensure customer and community confidence is maintained. In some cases, this is also necessary to meet legal or regulatory requirements. To protect customer information, an organisation should:

- Understand, document and abide by legal and regulatory obligations for protection of customer information *[R1.4]*;
- Apply strong access control and access logging to customer information resources *[R4.3 and 7.3]*;
- Educate customers on the protection of their own authentication credentials *[R6.2]*;
- Ensure service providers (e.g. backup, storage) provide a level of information security equivalent to that of the organisation *[R4.4]*; and
- Establish and publish a policy on the protection of customer information.

Recommendation 5.3: Assess the security of all organisations involved in the business value chain

The security of an interconnected network is only as strong as the weakest link. As a result, it is necessary for an organisation to take steps to ensure the security of their connected business partners is at a level equivalent to that internal to the organisation. Where required, organisations should assist connected nodes in achieving this level of information security through supporting security initiatives such as:

- Joint risk assessment and security testing exercises;
- Joint business continuity exercises;
- Security information sharing; and
- Incident response process definition.

In order to define and formalise the degree to which the external party is held accountable for information security, the organisation should formally document these requirements in SLAs where necessary. *[R4.4]*

Conversely, organisations also have a responsibility to ensure the security of "nodes" under their control is at a suitable level to maintain the overall security profile of the network.

Recommendation 5.4: Consider employee interests in the design of security systems

Organisations must seek to address employee needs in order to mitigate the insider threat to information security. It is important for an organisation to align information security requirements and objectives to employee needs and vice versa. Ensuring employees have

---

[43] Commonwealth of Australia, *Corporations Act 2001*, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/*

[44] Commonwealth of Australia, *National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000*, 2007, *http://www.privacy.gov.au/publications/npps01.html*

[45] Australian Securities Exchange, *Listing Rules Chapter 3 - Continuous Disclosure*, 2003, *http://www.asx.com.au/ListingRules/chapters/Chapter03.pdf*

appropriate incentives to understand and support information security in the organisation will enable a quicker and more effective take-up of the ‘culture of security’ It is through including employees in the security planning phases that an organisation can ensure employee buy-in on organisational goals and operations.

Relevant considerations in this area include the protection of:

- Employee personal information including payroll, address, dependents, employment history and other sensitive information; and
- Employee communications including email, telephone and mail correspondence.

Working with the human resources function, *[R2.4]* information security teams can address employee interests through the performance management cycle including:

- Involving employees in system design decisions where it may materially affect their needs;
- Encouraging employees to raise ad hoc concerns regarding information security; and
- Implementing internal processes to identify potential malicious insider behaviour early. *[R7.3]*

6. Information Security Requires Understanding and Commitment

Awareness of information security threats is critical to the ability of an organisation to manage risks. A high level of awareness within the organisation supports the development of a "culture of security" and can reduce the frequency and impact of information security incidents. A broad level of awareness is required for all staff, and a deep awareness and understanding is required for staff with key roles in information security.

Threat vs Vulnerability

A *threat* is defined as any potential circumstance, capability, action or event which could breach security or cause harm to an asset.

A *vulnerability* is a flaw or weakness in an information system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

A *risk* is an expectation of loss expressed as the probability that a particular *threat* will exploit a particular *vulnerability* with a particular harmful result.

Source: Adapted from Network Working Group, *RFC 2828*[46]

Information security awareness directly assists an organisation to:

- Develop a "culture of security" within the organisation's staff;
- Provide early detection for information security threats;
- Improve acceptance and use of the information security policy;
- Improve information security communication within the organisation;
- Effectively coordinate responses to information security incidents;
- Gain a whole of industry perspective on information security vulnerabilities and threats; and
- Achieve a high level of support for information security throughout the business functions.

Recommendation 6.1: Develop and maintain the information security policy to be practical and current

An information security policy should outline an organisation's interpretation of the information security principles and how they will be applied. The policy framework should reflect the tasks and responsibilities for information security which are key to good security governance. High-level policy statements applying the principles to the organisation's operations should be developed to be technology-neutral and enduring over time. These organisation-specific policies should provide a foundation for the ongoing evolution of security standards, baselines, guidelines and procedures to address current and future information security risks.

[46] Network Working Group, *Request For Comments (RFC) 2828 Internet Security Glossary*, 2000, *http://www.faqs.org/rfcs/rfc2828.html*

In order to achieve this, general requirements for information security policy should include:

- An annual review of policy statements;
- The use of clear and concise policy statements;
- The establishment of a policy exemption procedure; and
- Statements of compliance to the security policy from business partners.

Recommendation 6.2: Establish employee and contractor education and awareness programmes relevant to the organisation and individual roles

As employees have a key role in identifying information security risks and enforcing agreed controls, it is crucial for the organisation's information security principles to be communicated clearly and effectively to all staff. By embedding information security in "the way we do business", organisations can have greater confidence in the ability of all staff to make effective risk-based decisions. To develop and maintain this internal 'culture of security', education and awareness programs are especially important for new employees and contractors, and when there are material changes to the organisation's information systems, business operations, or risk profile.

US DoD 8570.1—Information Assurance Training, Certification, and Workforce Management

While specific to US defense department requirements, the United States *Department of Defense Directive 8570.1 – Information Assurance Training, Certification, and Workforce Management* provides a basis for an enterprise-wide solution to train, certify, and manage an Information Assurance workforce.

The directive requires Information Assurance technicians and managers to be trained and certified to a DoD baseline requirement. The Directive's accompanying Manual identifies the specific certifications mandated by the Directive's enterprise-wide certification program.

Source: US The United States Department of Defense[47]

Employee and contractor information security awareness and education programs should:

- Communicate the importance and relevance of information security to the organisation;
- Provide 'real world' examples or demonstrations of information security risk scenarios;
- Raise the awareness of current security threats and support the identification of such threats;
- Provide clear guidance on incorporating security considerations into day-to-day tasks *[R2.1]*; and
- Provide an avenue to address staff concerns regarding the impact of information security on their role and the operation of the business.

Awareness and education programs can be delivered in a variety of formats, which may include or be a combination of:

- Seminars;

- Training courses (either with a trainer or via eLearning);
- Group/team discussion meetings;
- Information security notices (both electronic and physical info-sheets and signage); and
- Coordinated exercises.

Meanwhile, staff with specific key responsibilities should be offered specialised security training. Organisations should consider the approach documented in the US Department of Defense (DoD) Directive 8570.1—Information Assurance Training, Certification, and Workforce Management[47], and resources such as the Asia-Pacific Economic Cooperation (APEC) Information Security Skills Certification Guide[48].

To ensure the most effective awareness programme, a variety of communication media can be used, with varying degrees of information richness, data capacity and response times (as shown in Table 7):

Communication Medium	Information Richness	Data Capacity	Response time
Face-to-face discussion	Highest	Lowest	Real-time
Telephone	High	Low	Real-time
E-mail	Moderate	Moderate	Real-time – Daily
Personalised note or memo	Moderate	Moderate	Daily
Individualised Letter	Moderate	Moderate	Few days
Formal written report	Low	High	Weekly or more
Flyer or bulletin	Low	High	Weekly or no response
Formal numeric report	Lowest	Highest	Weekly or more

- Information richness is the level at which the meaning intended by the information sender corresponds to the meaning received by the information recipient.
- Data capacity is the amount and / or the level of detail information can be communicated effectively via the medium.
- Response time is the time in which receivers will require to respond to the information sender in reply to the initial communication.

Table 7: Communication Mediums in the Workplace[49]

[47] The United States Department of Defense, *Directive 8570.1 – Information Assurance Training, Certification, and Workforce Management*, 2004, *www.amc.army.mil/amc/ci/matrix/downloads/DoD8570.1_MIATCWFM07-29-25.doc*

[48] Asia-Pacific Economic Cooperation, *Information Security Skills Certification Guide*, 2007, *http://siftsecurity.net/*

[49] Adapted from Gerloff 1984 as cited in Nelson and Quick, *Organizational Behavior 5th Edition*, South-Western College, 2005

Recommendation 6.3: Incorporate information security into existing communications processes

In order to address information security issues in a timely manner, clear and effective communication channels must coincide with a well informed workforce. To aid in the communication of information security threats and vulnerabilities, formalised procedures, associated forms and templates can assist staff in providing adequate and relevant information.

The inclusion of information security within existing processes—such as weekly news bulletins, position descriptions, change logs, and similar—can ensure that the issue is considered by all staff throughout the organisation.

Such communications mechanisms may include:

- Change management forms;
- Incident reporting forms;
- News bulletin email templates;
- Database of emails for key organisational contact points;
- Helpdesk hotline; and
- Pagers for security staff.

Meanwhile, resources such as helpdesk services and staff meetings provide an avenue to discuss information security concerns. *[R6.2]*

Furthermore, adequate structures should be implemented to aid in the communication of threats and vulnerabilities to external parties – such as investors, regulators and customers. *[R5.1~5.4]*

Case Study: Cyber-Storm—Inter-Organisation Exercises

Scenario Context

Cyber Storm, held in the US on February 6-10, 2006 was the first US Government led, full scale, cyber-security exercise of its kind. Cyber Storm coordinated effort between international, US federal and state governments, and private sector stakeholders to exercise their response, coordination and recovery in reaction to simulated cyber events. Australia participated in the US exercise through the Attorney-General's critical infrastructure protection branch.

Among the attendees were 100 public and private sector agencies, associations and corporations from over 60 locations and 5 countries. The exercise scenario simulated a large-scale cyber campaign affecting or disrupting multiple critical infrastructure elements within the Energy, Information Technology, Transportation and Telecommunications Sectors in the United States. The attacker used multiple electronic attack vectors, then exacerbated public and market response by encouraging and injecting misleading information in the media.

Developments

Despite the strength of individual organisations' capabilities in dealing with IT and cyber threats, the exercise showed how sophisticated threat examples across

multiple organisations and industries highlighted weaknesses and gaps in a coordinated response.

The US Government concluded eight findings from the exercises, including:

- Correlation of multiple incidents across multiple infrastructures and between the public and private sectors remains a major challenge; and
- A strategic communications and public relations plan must be an integral part of the contingency plan and response plan, in order to provide critical information to the response community and empower the public to take appropriate response actions.

Lessons Learnt

- Despite many organisations now having effective internal information security incident response capabilities, the ability to co-ordinate these across interlinked organisations is not yet mature. Organisations should engage in information security sharing and exercises with industry peers *[R6.4]*; and
- Communication of information security threats both internal and external enhances the ability for the organisation to respond to an incident. Organisations should ensure that the communications strategy for information security related tasks such as incident response is efficient and effective. *[R6.3]*

Further Information

www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf

www.computerworld.com.au/index.php/id;1387329132;fp;4;fpid;16

Case Study 8: Cyber-Storm—Inter-Organisation Exercises

Recommendation 6.4: Participate in informal and formalised information sharing networks

Information sharing allows organisations to enhance their understanding of current risks, best-practice defence methods and future trends by engaging in communications with other organisations in the same industry or with a similar risk profile. Such communication allows an organisation to more effectively identify deviation from industry norms which could indicate an attack or potential vulnerability.

Both informal (or *ad hoc)* information sharing networks—between peers in similar organisations—and formalised information sharing networks—such as the TISN—are of considerable value to critical infrastructure organisations. A formalised non-disclosure agreement may be required in some cases to share more sensitive information with greater confidence about its use and protection.

Information sharing arrangements can be considered for:

- Industry organisations—a group of enterprises from the same industry sharing information on security risks, threats and trends;
- Public/private associations and forums—groups including the TISN through which government and industry can share information on security risks, threats and trends related to critical infrastructure security interests;

- Critical service or product suppliers—a collaboration of key service providers to ensure risks and controls are consistently acknowledged by all parts of the supply chain; and
- Customers—ensuring that end-users are engaged in the security discussion.

Case Study: SCADA – Informal Information Sharing

Scenario Context

In 2004, the Information Technology Security Expert Advisory Group (ITSEAG) identified the need for a project across the Trusted Information Sharing Network (TISN) to collaborate on the security of Supervisory Control and Data Acquisition (SCADA) networks.

SCADA networks are widely used to monitor and control processes in the provision of essential services in Australia, including water, energy, transport, waste management and broadcasting.

Most SCADA systems were originally built before, and often separate from, other corporate networks – using their own protocols and little or no external connection to other systems. However, in seeking greater efficiency; access to critical operations data, remote access computing, better asset management and more timely corporate decision making, SCADA networks are increasingly being connected to corporate and business networks.

Developments

In late 2004, the ITSEAG supported the establishment of a SCADA Community of Interest (CoI). ITSEAG was able to bring together members of the respective sectors who use SCADA systems, in a forum with the aim to share information about SCADA security risks, threats and controls.

SCADA CoI workshops are held across Australia quarterly. They are free and open to owners and operators of critical infrastructure who have an interest in SCADA security, and include international and domestic speakers who are experts in the field of SCADA security. The group supports information sharing between users of SCADA systems, across industry and organisational boundaries, in the interests of security and risk management.

Lessons Learnt

- Organisations should seek to participate in informal and formalised information sharing networks such as the SCADA CoI to: *[R6.4]*
  - Support the discussion and resolution of systemic issues across organisational boundaries; and
  - Establish relationships to allow for cross-organisational incident response.
- Organisations should recommend key staff members with information security responsibilities to participate in information sharing in order to maintain their level of expertise in meeting the organisation's information security needs.

[R7.1]

Further Information

http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84E AA)~Vol+1+No+3.pdf/$file/Vol+1+No+3.pdf

www.scadacoi.com.au

http://www.engineersaustralia.org.au/shadomx/apps/fms/fmsdownload.cfm?file_uuid=C960676F-E935-DC91-E91E-5E5595A37ECF&siteName=ieaust

Case Study 9: SCADA—Informal Information Sharing

7. Information Security Requires Continual Improvement

As an organisation's risk exposure is dynamic, information security review and improvement must be a part of 'business as usual'. Good security governance will enable an organisation to manage the gap created by technology adoption outpacing controls adoption. Ongoing improvement allows the organisation to sustain the state of information security at a level which is acceptable to internal and external stakeholders, and maintains the organisation's risk at the appropriate tolerable level.

Continual improvement allows the organisation to:

- Maintain capabilities to assess security risks and implement effective controls;
- Provide assurance that information security risks are identified and managed consistently;
- Satisfy legal and regulatory requirements consistently;
- Ensure security considerations are included in the selection and adoption of new technology; and
- Audit the organisation's performance over time.

Recommendation 7.1: Ensure information security expertise and experience is available to meet the organisation's needs

It is crucial for all organisations to maintain access to sufficient expertise and experience to enable required information security tasks to be completed competently. Personnel with the necessary expertise and experience may be either internal to the organisation, or external via a formalised service provider agreement. Key roles within the organisation that will influence the security strategy and also the execution of the security strategy (including system designers, architects, administrators and owners) should maintain an appropriate currency of knowledge in the area of information security.

Consequently, staff with a specific role in the area of information security should be required to keep current with:

- Security technologies, threats and vulnerabilities;
- Changes in architecture design best practices (see Security Architecture Development); and
- Developments in business enabling technology solutions.

To achieve this, the organisation can:

- Incorporate these responsibilities within the job description of technical roles *[R4.2]*;
- Brief technical staff on strategic changes to the business to gain an understanding of the potential for security implications arising from these changes *[R6.3]*; and
- Allocate resources for technical staff to attend conferences, subscribe to forums and industry associations, as well as internal information sharing arrangements to enhance knowledge development *[R6.4]*.

Where technical capability is acquired via a service provider (vendor, consultant or contractor), the organisation should ensure that:

- Service providers are vetted through background and reference checks;
- Services provided are covered by non-disclosure agreements; and
- All communications are conducted securely.

Recommendation 7.2: Review information security controls against national and international standards

Regular review of information security policies, procedures and technical configurations ensure the state of information security is maintained in line with an organisation's objectives. This validates that the current information security plan is being achieved, and provides a basis for future planning. *[R1.2]*

To assess the state of information security an organisation can:

- Review information security policy to ensure high level objectives and policy statements are still relevant to the organisation's business drivers *[R6.1]*;
- Perform technical audits of information systems to verify known vulnerabilities are not present and risks continue to be mitigated to acceptable levels; and
- Conduct periodic risk assessments that validate existing mitigation practices, and assess the impact of changes in the organisation or system's risk profile or external threat environment. *[R3.1]*

The duration between reviews should be determined by considering:

- Legal and regulatory requirements, including integration with audit and other internal/external risk reporting periods *[R1.2]*;
- The cost of conducting the review; and
- Changes in the external environment, including the prevalence of incidents/attacks in the industry, and threat levels as communicated by information sharing. *[R1.4]*

Case Study: ANAO—Government IT Security Audit

Scenario Context

In 2006, the Australian National Audit Office (ANAO) conducted audits of eight government agencies on the state of their IT Security.

The audit of each agency examined the framework for the effective management and control of IT security, including the management of IT operational security controls. Where applicable, this was conducted based on the Australian Government protective security and information and communications technology (ICT) security guidelines.

Developments

ANAO found that:

- Agencies were aware of Australian Government policies, practices and procedures for the protection of information. However, most did not align IT

security policy with risk management and government policy, practices and standards;

- Agencies were aware of external compliance obligations and IT staff were aware of relevant legislation. However only two agencies could demonstrate suitable processes to assess system compliance with their IT security policy;
- Most agencies did not maintain key IT operational procedures and configuration documentation. This was particularly evident of agencies that had contracted to third party service providers for the provision of IT and / or IT security services; and
- A number of other opportunities for further improvement in agencies' policies and procedures relating to IT security management practices were also found.

Lessons Learnt

- Awareness of legal and regulatory requirements must evolve into the development and implementation of suitable information security initiatives to support these requirements *[R1.4]*;
- Organisations should implement information security risk management in line with their enterprise risk management program, such that risk management drives information security. *[R3.1]*;
- Organisations should ensure end-to-end assignment of security responsibilities for information security throughout the business value chain *[R4.4 and 5.3]*; and
- Organisations should periodically assess their level of information security compliance in the context of national and international standards. *[R7.2]*

Further Information

www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf

www.dsd.gov.au/library/infosec/acsi33.html

Case Study 10: ANAO—Government IT Security Audit

Recommendation 7.3: Implement systems and processes to identify and respond to malicious or unintended information security breaches

Malicious or poorly trained end users can present a significant security risk to any information system. As a result of the key part end users play in an information system, all user activity with relevance to an organisation's information security (including access and use of sensitive information assets) should be monitored and subject to audit. Organisations must align such monitoring with legal and industry regulations.

To realise effective incident detection an organisation can:

- Log user access and rights modifications, with a focus on privileged or administrative access levels;
- Deploy intrusion detection or prevention systems, or system integrity verification software, to alert system managers of unauthorised access or usage;

- Ensure sufficiently trained personnel are available to complete investigations if unauthorised access or usage is suspected; and
- Develop effective incident escalation procedures to enable immediate response.

Case Study: Removable Media Devices

Scenario Context

Removable media devices (including USB data keys, flash and hard drives, mp3 players, mobile phones and cameras) are becoming smaller in physical dimensions whilst increasing memory storage capacity. USB keys in particular have become extremely popular for transferring large amounts of data to aid business operations. These keys are perceived to be safe due to their widespread popularity. They are commonly presented as a complimentary gift at industry conferences or as buying incentives. Recently in the United Kingdom, in a social engineering experiment designed to test their client's IT security, consultants put self running malicious code on USB devices and spread them in a company car park. The malicious code collected sensitive information from the employees' computers and sent it to the consultant's email. Of the 20 USB drives planted, 15 were found by curious employees and connected to the organisation's computers almost immediately. The information collected could have allowed the compromise of other systems within the organisation's network.

Developments

Survey results worldwide have shown organisations have not protected themselves against attacks like this. In the United Kingdom, the Department of Trade and Industry (DTI) 2006 Information Security Breaches Survey found that 55% of firms have taken no steps to protect themselves against the threat posed by removable media devices. Similarly, AusCERT found only 50% of organisations utilised management of removable computer media policies and procedures in Australia. Changing system configurations to inhibit or restrict usage and encrypting of data are both rarely used.

Lessons Learnt

- The application of controls such as disabling of drives and ports, encryption of files, applying malware protection and disabling autorun should be applied wherever suited for the business requirement. The selection of controls should be preceded by a detailed risk assessment; *[R3.2]*;
- Approved removable media device enforcement is vital and individuals must be held accountable for the use and safety of approved devices; *[R4.1]*;
- Education on the threats of removable media should be provided to all staff. *[R6.2]*; and
- All staff should be charged with the responsibility to be vigilant and ensure breaches are communicated as soon as possible. Technical monitoring of usage should be employed where possible. *[R7.3]*.

Further Information

www.dti.gov.uk/files/file28343.pdf

www.auscert.org.au/images/ACCSS2006.pdf

www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1112458,00.html

Case Study 11: Removable Media Devices

Recommendation 7.4: Develop a feedback process to incorporate incident details into risk assessments and control selection as part of the systems lifecycle

As a final step to the management of information security incidents, the organisation should complete a "Post Incident Review" (PIR) to formally capture and assess the root cause of the incident, remediation techniques used and future actions which can be used to prevent the incident or improve the response. The goal of this exercise should be to build the incident experience into the organisation's knowledge and operations.

Effective post-incident activities include:

- Meeting with incident handling personnel, information security, system and business owners to discuss the speed with which the incident was identified, the response determined and implemented, and the effectiveness of the response;
- Capturing incident and response details within a "Post Incident Report", to be circulated to a controlled group for considering appropriate procedural or policy level changes arising from the incident;
- Acknowledging relevant past incident information and applying recommendations to the design and development of new systems;
- Using incident reports as an input to regular information security policy, standards and procedure review sessions; and
- The integration of incident data into governance reporting.

Recommendation 7.5: Include security as a selection criteria for assessing new technologies and applications for the organisation

It is often accepted that legacy systems will not have the same level of security as newer systems. However, such an acceptance requires that when these systems are subject to upgrade or replacement, security is included as a selection criteria for the new system. Ignoring the cost of ensuring that security is built in to a system from the start, may skew the business case assessment of the system's value.

In order to securely adopt new technologies, organisations can:

- Consider security at the conception and design stage of the adoption process *[R2.5]*;
- Adopt trusted and open standards as guidelines for design and management *[R2.6]*; and
- Have a formal process of documenting the security requirements for new systems, and include this as an element of "Request For Proposal" (RFP) documents for response from vendors. *[R4.4]*

Security Architecture Development

Having identified and developed the Principles of Information Security in the previous section, it is now necessary to consider the practical application of these Principles to the development of the Enterprise Architecture. Recommendation action items as identified in the previous section are applied specifically to Enterprise Architecture components as part of each phase of the TOGAF Architecture Development Method (ADM)[7] to demonstrate how a Security Architecture[8] can be developed (the ADM Cycle is shown in Figure 12).

At each phase, relevant considerations of the Principles will be discussed along with practical applications of these principles. Tables are provided for each phase to clearly indicate the recommendations used in an easy to use manner.

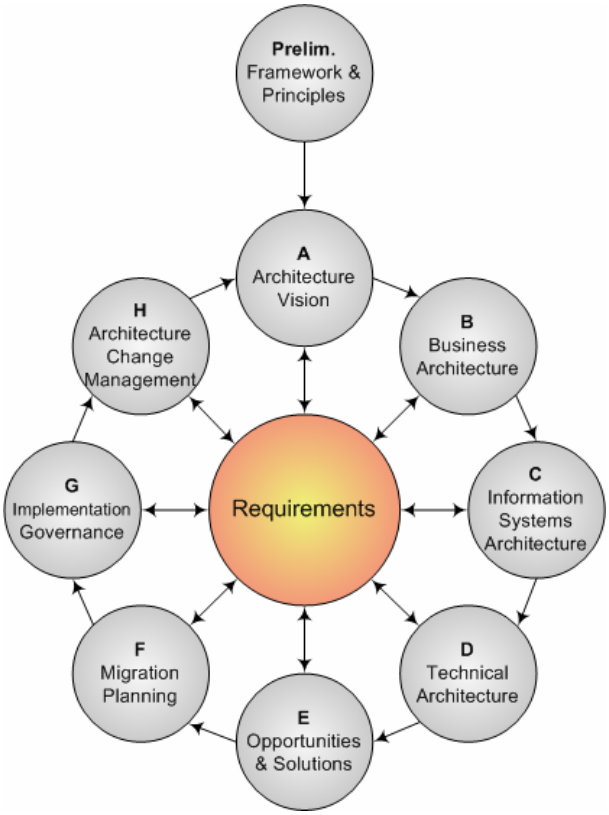


Figure 12: The Enterprise Architecture Development Cycle

While convergence of technologies changes and influences Enterprise and Security Architecture, it does not change the underlying processes used to develop them. Furthermore, as the effects of convergence become more apparent, the use of governance-level security principles can ensure the Security Architecture remains enforceable, measurable and continues to adequately protect the organisation.

Throughout the following sections, which follow the order of the ADM phases as illustrated in Figure 12, a number of technical studies are provided to illustrate with current convergence scenarios, how the challenges of convergence can be handled within Enterprise Architecture.

Preliminary Phase: Framework and Principles

Prior to entering the Enterprise Architecture development cycle, the governing process and principles must be established. The Principles outlined in the previous section provide a suitable starting point in the Security Architecture effort.

During the preliminary phase, consideration must be given to the following:

- Typically the Enterprise Architecture team will have little experience defining and understanding security requirements. Therefore, a security architect should be appointed to provide specific guidance to the team *[R4.2]*; and
- To establish context, a list of external regulatory and other stakeholder requirements should be defined *[R1.4]*. These can be developed into specific information security requirements for analysis and implementation later in the process.

No.	Recommendation
1.4	Ensure information security supports legal and regulatory compliance requirements
4.2	Assign information security responsibilities throughout the organisation

Table 8: Recommendations Applicable to the Preliminary Phase

Phase A: Architecture Vision

The objective of this phase is to garner support for the execution of the latest iteration of Enterprise Architecture development and establish its objectives. The architecture vision is intended to scope and shape subsequent phases.

During the architecture vision phase, consideration must be given to the following:

- The Security Architecture vision should clearly state how information Security Architecture supports the enterprise mission to prevent future misalignment. *[R1.1]*;
- Given that security is often viewed as a hindrance, managerial and executive support is required to achieve secure architecture outcomes. This can be achieved through the demonstration of information security benefits to executive management *[R1.3, R4.1, R5.4]*;
- The business is fundamentally supported by Enterprise Architecture. To ensure the architecture is stable and available, information systems continuity plans should be developed, documented, and tested *[R5.1]*; and
- A context for Security Architecture should be documented. This might include the definition of the current physical, business and regulatory environments *[R2.3]*.

No.	Recommendation
1.1	Develop information security strategy consistent with the business goals and responsibilities of the organisation, with Board-level

No.	Recommendation
	approval
1.3	Executive management should demonstrate support for enterprise information security at all levels of the organisation
2.3	Consider physical security aspects of information protection within "information security"
4.1	Hold executive management accountable for the state of enterprise information security
5.1	Implement information security controls to support service continuity
5.4	Consider employee interests in the design of security systems

Table 9: Recommendations Applicable to the Phase A

Phase B: Business Architecture

The objective of this phase is to describe the current Business Architecture of the organisation and subsequently also define a target architecture.

During the Business Architecture phase, consideration must be given to the following:

- Documenting Business Architecture facilitates the role of information security in addressing business goals *[R1.1]*;
- Assessing the risk of security failures in business processes can shape an organisation's target architectures and treatments of those risks *[R3.1]*. A cost / benefit analysis can determine which security mechanisms are the most appropriate for implementation *[R3.2]*;
- As business processes are identified and documented, so should their legitimate users (including products, services, and processes) and roles *[R4.2, R4.3, R4.4]*. This will ensure the appropriate accountability can be assigned and contracted; and
- Identifying external parties and dependant processes can help to validate that the Security Architecture supports both internal stakeholders *[R5.4]* and external stakeholders *[R5.1, R5.3]*. Furthermore, service level agreements can be established to ensure external parties do not undermine internal controls *[R4.4]*.

No.	Recommendation
1.1	Develop information security strategy consistent with the business goals and responsibilities of the organisation, with Board-level approval
3.1	Conduct information security risk assessments in line with the enterprise risk assessment methodology
3.2	Prioritise the treatment of risks and ensure the treatment is

No.	Recommendation
	proportionate to the business impact
4.2	Assign information security responsibilities throughout the organisation
4.3	Allocate responsibility for information security to match business roles
4.4	Define information security responsibilities for external parties in the engagement contract
5.1	Implement information security controls to support service continuity
5.3	Ensure the security of all organisations involved in the business value chain
5.4	Consider employee interests in the design of security systems

Table 10: Recommendations Applicable to the Phase B

Technical Study: Business Process Outsourcing

Business process outsourcing refers to an arrangement by which business tasks that would otherwise be performed by staff internal to the organisation are transferred to specialist external entities. As the components of the Business Architectures of many organisations converge at a single outsourcer, significant implications for Business Architecture arise as potentially crucial business processes are being performed by third parties.

How does convergence impact on Business Architecture?

Outsourcing necessarily involves changes to organisational boundaries and can lead to a number of information security issues as business activities are conducted over third party infrastructure or processing handed to a third party. As a result, there exists a shared responsibility for information security between an organisation and its outsourcers. The challenge is defining exactly where this individual responsibilities and accountabilities lie in various scenarios.

How can information security principles be applied to secure the changed architecture?

In line with Principle 4 'Information Security Accountabilities Should be Defined and Acknowledged', an organisation should define information security responsibilities for outsourcers and enforce these responsibilities through legal or contractual arrangements such as service level agreements (SLAs). Such responsibilities and accountabilities typically include minimum requirements for:

- Data protection—Where does one organisations responsibility end and the others begin? If data is lost or stolen, who should be notified?
- Access control—Which users and business units have access to which functions?

Who and how will this be enforced?

- Auditing—Who has responsibly for auditing which components? When will audits be conducted and who will bear the cost of remediation? and
- Incident response—Who is responsible for each stage of incident response? How will activities be co-ordinated?

Furthermore, an organisation outsourcing core business activities should seek to retain management control of processes to enable timely and appropriate response to issues that may arise.

Technical Study 1: Business Process Outsourcing

Phase C: Information Systems Architecture

The goal of this phase is to develop target Information and Application Architectures to support the Business Architecture.

During the Information Systems Architecture phase, consideration must be given to the following:

- Enterprise Architecture aims to achieve business modularity and flexibility. Often this is only possible through standardisation of data, applications and protocols. Similarly, security standards and guidelines that are tested, proven and reliable should be selected *[2.6, R7.2]*;
- Information assets that are identified should be classified in accordance with an Information Classification Policy in order to determine the level of protection required *[R5.2]*;
- Important events and actions for logging should be identified and documented so unauthorised behaviour can be detected *[R7.3]*;
- Once assets have been identified, threat modelling can be undertaken to enumerate attack vectors and potential threats to those assets *[R3.1]*. This is essential to understanding how the assets can be protected; and
- A significant component of the Information Systems Architecture process is identifying the application interactions. Documenting these along with any assumptions made about security can prevent inadvertent breach of policy or best practice by security architects and implementation staff *[R2.5]*.

No.	Recommendation
2.5	Embed information security within the lifecycle of enterprise information systems
2.6	Implement security based on transparent, trusted and proven solutions
3.1	Conduct information security risk assessments in line with the

No.	Recommendation
	enterprise risk assessment methodology
5.2	Ensure sensitive customer and community data is protected appropriately
7.2	Review information security controls against national and international standards

Table 11: Recommendations Applicable to the Phase C

Technical Study: Service Oriented Architecture

Service oriented architecture (SOA) is an information systems design based on loosely coupled software services built to support seamless business process interactions. This form of architecture allows system components to be reused for many different applications, reducing development time and cost. It can also remove organisational borders, enabling seamless interaction with customers, suppliers and clients (i.e. courier and transport industries).

While the implementation of an SOA focuses change on an organisation's information systems architecture, it affects significant aspects of the entire Enterprise Architecture and requires consideration at all architecture layers.

How does convergence impact on Information Systems Architecture?

The industry-accepted best practice model of information systems architecture is changing from standalone applications with proprietary links to other applications, to one with interconnected application components (i.e. SOA).

Commonly, SOA is implemented using specific technologies such as:

- Data definition and representation using eXtensible mark-up language (XML);
- Communications over internet protocol (IP); and
- Application component linkage using web services (WS).

As a result of the move to distributed components, external and internal parties are no longer required to prove their identity to a single system, but rather a large number of dispersed system components. This presents the challenge of maintaining security throughout the interconnected system, without requiring the execution of complicated security processes at each component.

How can information security principles be applied to secure the changed architecture?

As SOA technologies can incorporate the integration of components throughout an enterprise or even across an entire supply chain, applying open and trusted security standards – as identified by Principle 2 'Information Security Impacts on the Entire Organisation' – will help to ensure that security considerations are addressed consistently.

Establishing an SOA across the enterprise will typically involve implementing:

- Federated identity security based on the security assertion mark-up language (SAML) to ensure all entities are authenticated and don't exceed their access rights; and
- Message security based on WS security to ensure sensitive information is never exposed unnecessarily.

Further information:

SAML Standard

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

WS-Security Standard

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

Technical Study 2: Service Oriented Architecture

Phase D: Technical Architecture

The goal of this phase is to develop a target Technical Architecture to support the information and Application Architectures.

During the Technical Architecture phase, consideration must be given to the following:

- The Technical Architecture, particularly in Critical Infrastructure organisations must be highly available. To achieve this, redundancy, backup and other continuity solutions should be incorporated into Technical Architecture *[R5.1]*. Denial of service attack protection, detection and prevention mechanisms should also be considered[8];
- A Technical Architecture will require monitoring to detect any security incidents or failures within the architecture *[R7.3]*. This can often be achieved by adding application and system logging, intrusion detection, and centralised event correlation;
- The regulatory environment or the criticality of business data creates protection requirements on information used by an organisation *[R5.2]*. In a Technical Architecture this can be achieved through encryption mechanisms in storage (e.g. database encryption) and transit (e.g. SSL/TLS), as well as integrity mechanisms (e.g. message hashes);
- Particularly important in interconnected architectures is the concept of authentication. The identity of internal and external users and systems should be known throughout the Technical Architecture *[R4.3]*. A centralised identity management solution can be used to provide single sign-on and identity verification as required;
- To prevent a compromise of one technical component from affecting others and to limit the impact of any security incident, all network, system, application, and user components should be designed to operate with the least privileges possible to complete their business goals *[R4.3]*; and

- Implementing standards and protocols that are considered by the wider community to be secure can increase security and decrease time-to-market. Furthermore, using open standards facilitates interoperability in modular architectures *[R2.6]*.

No.	Recommendation
2.6	Implement security based on transparent, trusted and proven solutions
4.3	Allocate responsibility for information security to match business roles
5.1	Implement information security controls to support service continuity
5.2	Ensure sensitive customer and community data is protected appropriately
7.3	Implement systems and processes to identify and respond to malicious or unintended information security breaches

Table 12: Recommendations Applicable to the Phase D

Technical Study: Flexible Infrastructure

Flexible infrastructure refers to networking technologies that can be adapted to carry many forms of data and support several business functions. This reduces overheads in maintaining multiple single-purpose infrastructures and eases operational knowledge and skill requirements.

How does convergence impact on Technical Architecture?

Previously, many network infrastructures were deployed to support a single function such as voice communications. Today many of these infrastructures are converging on a single Internet Protocol (IP) based network, capable of generically handling any form of data.

Moving many systems to a single infrastructure creates a strong dependency on that infrastructure. No longer does a failure cause an outage in one system, rather it causes an outage in all systems. This is further compounded by the fact that outages in some critical infrastructure services such as telephone communications can have more severe effects than others.

Given that different systems which may be processing and transferring data of different classification levels share infrastructure, the risk that the compromise of one system will result in the compromise of other systems and their communications increases. Moreover, all the potential attackers of one system become potential attackers of all systems sharing the infrastructure[10].

How can first principles be applied to secure the changed architecture?

In order to protect customer and other sensitive information travelling across a shared

network, as per Principle 5 ‘Information Security Must Consider Internal and External Stakeholders,’ virtual private network (VPN) technology can provide low-level encryption for each individual purpose without affecting specific applications. Provisioning redundant and independent infrastructure components such as Internet feeds, routers, firewalls, and power supplies will prevent a single failure from causing an architecture-wide outage.

Technical Study 3: Flexible Infrastructure

Phase E: Opportunities and Solutions

During this phase, various implementations identified in the development of a target architecture are evaluated and selected. A strategic means of implementing the changes is also identified.

During the opportunities and solutions phase, consideration must be given to the following:

- A part of the assessment of proposed architectures, the risk profile of each should be evaluated and compared. Where two or more architectures achieve business objectives equally, the one with the lowest risk profile should be considered preferable *[R3.1]*; and
- There is a risk of over-complicating a security architecture which can be overcome in the selection process by identifying solutions which are proportionate to organisational risk *[R3.2]*. Identification requires risks assessments to be carried out at business, information, application and technical levels *[R3.1, R7.4]*.

No.	Recommendation
3.1	Conduct information security risk assessments in line with the enterprise risk assessment methodology
3.2	Prioritise the treatment of risks and ensure the treatment is proportionate to the business impact
7.4	Develop a feedback process to incorporate incident details into risk assessments and control selection as part of the systems lifecycle

Table 13: Recommendations Applicable to the Phase E

Phase F: Migration Planning

Migration planning is the detailed specification of what architecture components will be implemented and the scheduling of supporting tasks.

During the migration planning phase, consideration must be given to the following:

- The transitional architecture will impact on the current baseline architecture. From a security perspective, this impact should be assessed to ensure the security of the entire architecture is not compromised during migration *[R3.1]*. As part of the risk mitigation strategy, the efficacy of security measures should be regularly tested during migration *[R7.5]*; and

- Architecture changes may impact on the way an organisation does business. Any such changes should be disseminated to relevant stakeholders and affected parties to ensure business operations continue to function efficiently *[R6.4]*.

No.	Recommendation
3.1	Conduct information security risk assessments in line with the enterprise risk assessment methodology
6.4	Participate in ad-hoc and formalised information sharing networks
7.5	Include security as a selection criteria for assessing new technologies for the organisation

Table 14: Recommendations Applicable to the Phase F

Phase G: Implementation Governance

Implementation governance is concerned with the monitoring of architecture change in order to ensure that the target architecture is implemented as specified.

During the implementation governance phase, consideration must be given to the following:

- In order to verify the Security Architecture has been implemented as required, regular reviews and testing should be conducted, particularly during transitional states *[R7.2]*. This will include framework audits against such standards as *ISO 27001* and technical assessments such as code reviews and penetration tests; and
- When a security incident occurs, conducting a root-cause analysis will allow an organisation to determine if the incident was the result of a fault in the implementation of the security architecture *[R7.4]*.

No.	Recommendation
7.2	Review information security controls against national and international standards
7.4	Develop a feedback process to incorporate incident details into risk assessments and control selection as part of the systems lifecycle

Table 15: Recommendations Applicable to the Phase G

Phase H: Architecture Change Management

This phase is responsible for determining if further architectural change is required and when the cycle should begin afresh.

During the architecture change management phase, consideration must be given to the following:

- As the Enterprise Architecture changes, the Security Architecture protecting it must also evolve. A periodic review of Security Architecture will ensure that current controls

continue to provide an adequate level of security or identify areas of potential weakness *[R7.2]*;

- The external threats to an organisation are ever-changing, with new attack techniques and vulnerabilities emerging on a daily basis. To counter the changing threat landscape, internal research and awareness programmes *[R6.1, R6.4]* can be established in addition to strong patch management processes *[R2.2, R2.5]*; and
- Monitoring user activity can assist in determining when the baseline security architecture begins to become ineffective and can be used as a catalyst for change *[R7.3]*. Similarly, when security incidents occur, it is important to conduct root cause analysis and initiate architectural change if required *[R7.4]*.

No.	Recommendation
2.2	Implement enterprise processes that support practical and timely solutions for information security
2.5	Embed information security within the lifecycle of enterprise information systems
6.1	Develop and maintain the information security policy to be practical and current
6.4	Participate in informal and formalised information sharing networks
7.2	Review information security controls against national and international standards
7.3	Implement systems and processes to identify and respond to malicious or unintended information security breaches
7.4	Develop a feedback process to incorporate incident details into risk assessments and control selection as part of the systems lifecycle

Table 16: Recommendations Applicable to the Phase H

Technical Study: Merger or Acquisition

A merger or acquisition of another organisation will typically be a catalyst for major changes in organisational architecture. The integration of two completely disparate organisational structures and supporting infrastructures will commonly result in significant changes to architecture components, including:

- Widening of organisational borders;
- Unification of business structure;
- Integration of business processes; and
- Merging and interoperation of technology components.

How does convergence impact on Architecture Change Management?

The convergence trend has brought about Enterprise Architecture that supports a greater number of activities and purposes using multipurpose infrastructure. As a result of this, changes to the architecture potentially affect a larger number of business units and users.

Organisations with converged architectures will have a greater need for in-depth impact analysis in order to establish information security risks that may arise during or after the implementation of architectural changes. In particular, the integration of two converged architectures may pose a number of challenges to the establishment of a usable and reliable architecture that meets the needs of the newly-formed organisation.

How can first principles be applied to secure the changed architecture?

By assessing the security implications of integrating two organisational architectures, organisations involved in a merger or acquisition can develop the resulting architecture in a manner that minimises information security risks.

This will commonly involve applying Principle 2 ‘Information Security Impacts on the Entire Organisation’, Principle 6 ‘Information Security Requires Understanding and Commitment’, and Principle 7 ‘Information Security Requires Continual Improvement’ by conducting a series of tasks throughout the merger or acquisition process. These tasks will include:

- Assessing the security expertise and experience levels of staff from both organisations to ensure knowledge and skill sets meet the information security demands of implementing the merger or acquisition;
- Considering an organisation’s posture, employee education and policies in the area of information security to identify areas that may not integrate smoothly with the other organisation’s structure;
- Identifying security technologies to be kept or discarded for the final integrated architecture;
- Identifying and assessing information security risks that may result from the merger or acquisition and implementing appropriate mitigation strategies such as new security technologies or processes;
- Conducting a post-implementation security audit or test of the integrated architecture; and
- Initiating relevant employee training associated with the new organisation architecture, new policy framework and new technology structure.

Technical Study 4: Merger or Acquisition

Appendices

Appendix A: Principle Application in Addressing Convergence Challenges

The following table shows which Principle—when applied effectively—can be used in addressing the convergence challenges identified.

Convergence Challenges	**Principles of Information Security**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
Unauthorised Functionality		✓	✓			✓	
Availability of Service	✓	✓	✓		✓	✓	✓
Confidentiality, Integrity, and Privacy	✓	✓	✓				✓
Authentication and Authorisation			✓	✓	✓		✓
Increased Attack Surface		✓	✓		✓		
Responsibility and Accountability		✓	✓	✓	✓	✓	✓
Incident Detection and Response			✓	✓	✓	✓	✓

Appendix B: Mapping of Principles to Existing Publications

The following tables show the mapping of the Principles of Information Security presented in this paper against a number of existing information security standard sets. The ticks in these diagrams indicate which of the Principles of Information Security in this paper (number 1–7 at the top), address the corresponding Principles in the earlier work (detailed in the left column).

NIST—Generally Accepted Principles for Securing Information Technology Systems	**Principles of Information Security**						
	1	**2**	**3**	**4**	**5**	**6**	**7**
1. Computer Security Supports the Mission of the Organization	✓						
2. Computer Security is an Integral Element of Sound Management		✓	✓	✓	✓		
3. Computer Security Should be Cost Effective	✓		✓				
4. System Owners Have Security Responsibilities Outside Their Own Organization					✓		
5. Computer Security Responsibilities and Accountabilities Should be Made Explicit				✓			
6. Computer Security Requires a Comprehensive and Integrated Approach		✓					
7. Computer Security Should be Periodically Reassessed							✓
8. Computer Security is Constrained by Societal Factors					✓		

OECD—Guidelines for the Security of Information: Towards a Culture of Security	Principles of Information Security						
	1	2	3	4	5	6	7
1. Awareness						✓	
2. Responsibility				✓			
3. Response					✓		
4. Ethics					✓		
5. Democracy					✓	✓	
6. Risk Assessment			✓				
7. Security design and Implementation		✓					
8. Security Management		✓	✓		✓	✓	
9. Reassessment							✓

ISSA—Generally Accepted Information Security Principles	Principles of Information Security						
	1	2	3	4	5	6	7
1. Accountability				✓			
2. Awareness						✓	
3. Ethics					✓		
4. Multidisciplinary		✓			✓		
5. Proportionality			✓				
6. Integration		✓					
7. Timeliness						✓	
8. Assessment			✓				✓
9. Equity				✓		✓	

TISN—Leading Practices and Guidelines for Enterprise Security Governance	Principles of Information Security						
	1	2	3	4	5	6	7
1. Accountability				✓			
2. Awareness						✓	
3. Compliance							✓
4. Effectiveness	✓	✓					
5. Ethics					✓		
6. Inclusion		✓			✓		
7. Transparency	✓	✓	✓				
8. Measurement and Reporting			✓				✓
9. Scope		✓		✓	✓		
10. Response					✓		
11. Risk Management			✓				

Appendix C: Principle Self-Assessment Checklist

Pri-ID	Principles	Rec ID	Recommendations	Validation Items
1	Information Security Is Integral to Enterprise Strategy	1.1	• Develop information security strategy consistent with the business goals and responsibilities of the organisation, with Board-level approval	Information security strategy considers the input of stakeholders
				Information security strategy provides a clear statement of how security supports enterprise mission
				The information security governance program seeks to achieve the information security strategy
				Training and awareness programs are provided for enhancing information security acceptance
				Information security investment is allocated efficiently on the basis of quantitative analysis
				All organisational intellectual property is accounted for and protected
		1.2	• Ensure consistency of information security planning with strategic and operational planning	Long term information security planning supports the organisation's mission and long term strategy by minimising losses, protecting brand and competitive advantage
				Short term planning supports organisation's objectives and short term strategy by controlling project risks and managing vulnerabilities
		1.3	• Executive management should	Ultimate responsibility for the state of enterprise information security lies with executive management
				Security is incorporated into the project development process

			demonstrate support for enterprise information security at all levels of the organisation	Information security policies and standards are applicable to executive management
		1.4	• Ensure information security supports legal and regulatory compliance requirements	Legal, Audit or Risk department is supported by the Information Security Team in determining appropriate information security implications of regulations
				Metrics are developed and used for validation of compliance requirements
2	Information Security Impacts on the Entire Organisation	2.1	• Include representatives of all areas of the organisation in information security decision making	The information security steering committee (or equivalent) comprises of representatives of key stakeholder groups and reports to CEO / board
				Periodic internal stakeholder workshops are held for information security
				Business units are required to state compliance to information security policies periodically
		2.2	• Implement enterprise processes that support practical and timely solutions for information security	Business stakeholders provide an “impact statement” of proposed security standards, procedures and guidelines upon review.
				Information security communications use suitable language
				Emergency change request and exception handling processes are used to administer and formalise stop-gap fixes
				Tested, proven and reliable information security solutions are considered first
				Escalation channels are present for expeditious approval for changes and exceptions

				Accountability for interim fixes and responsibility for providing a formal solution are assigned
				Training of staff on information security issues and their responsibilities is provided
		2.3	• Consider physical security aspects of information protection within "information security"	Enterprise security strategy including IT and physical security components
				Security officers have responsibility for both physical and information security
				Change requests review both physical and information security elements
		2.4	• Engage Human Resources to ensure people are managed as a component of information security within the organisation	Human Resource conducts adequate security background checks to validate suitability of prospective employees
				Security training is integrated into the induction process, physical and information access is uniformly granted.
				Human Resources maintains personnel security risk at an accepted level through: • Performance management; and • Awareness and exercises.
				Human Resources coordinates the removal of access rights upon employee dismissal or departure in a timely manner
		2.5	• Embed information security within the lifecycle of enterprise information	Security impacts of system design are documented and communicated during the concept phase
				Information system functional design requirements includes a 'security requirements specification' component
				Rigorous security testing is executed prior to production deployment

			systems	Exception procedures are implemented for non-compliant components (this includes a timeline and path for resolution)
				Vendor evidence of product security is requested and evaluated when considering proprietary solutions
				Security of information is maintained throughout the information lifecycle (i.e. creation, processing, storage, deletion and destruction)
				Periodic assurance audit and testing plan for information systems is developed and maintained
				Destruction and decommissioning of computer media is conducted in line with best practices such that no sensitive information remains
		2.6	• Implement security based on transparent, trusted and proven solutions	Trusted and proven security management standards such as ISO 17799 / PCI DSS—are used or considered when designing security
				Independently evaluated vendor products under programmes such as Common Criteria—are used or considered when implementing information systems
				Trusted and proven information system development processes such as ITIL, OWASP and CIS (see page 44 for a definition)—are used or considered when developing information systems
				Open encryption algorithms such as AES (see page 44 for a definition)—are used or considered when utilising authentication or storage mechanisms for information
		2.7	• Implement layered security	Physical, personnel and IT security programs align to provide protection the organisation against security risks
				Separation of duties is enforced at both a personnel and system level
				Technical, procedural and operational controls for information security are implemented and are aligned
				Redundancy and contingency plans are part of the business continuity program.

				Security control failures are assessed and secondary controls are in place
3	Enterprise Risk Management Defines Information Security Requirements	3.1	• Conduct information security risk assessments in line with the enterprise risk assessment methodology	Information security risk assessments consider a comprehensive scope of risks
				The security risk management methodology is consistent with the enterprise risk management methodology
				Information security risk assessments are reviewed by Group Audit or Group Risk to assess rating consistency between domains
				Reporting for information security is in line with enterprise risk management standards
		3.2	• Prioritise the treatment of risks and ensure the treatment is proportionate to the business impact	Information asset and risk register is in place and is developed with assistance from the risk management team
				Method for materially comparing information security risks and their treatments is developed with assistance from the risk management team
				Information security risk schedule and resolution plan easily incorporates into enterprise level risk tracking by the enterprise risk management team
				Risk mitigation activities are monitored to ensure they are appropriate and proportionate to the business impact
4	Information Security Accountabilities Should be Defined and Acknowledged	4.1	• Hold executive management accountable for the state of enterprise information security	Enterprise information security is structured to be in line with the enterprise mission and strategy
				Information security is a key risk management and internal control mechanism
				Information security responsibilities are delegated throughout the organisation and effective escalation and reporting mechanisms are in place.
				Information security performance is a component of key performance indicators (KPIs) for executive management roles
		4.2	• Assign information	Separation of duties is implemented to provide additional checks and balances to deter and detect malicious activity

			security responsibilities throughout the organisation	Technical responsibility for information security is assigned to the IT department
				Human Resources department is a key stakeholder in the definition of employee responsibilities, education and awareness initiatives in the area of information security, as well as monitoring of employee behaviour
				A security architect is appointed within the Enterprise Architecture team
				All staff are provided with the necessary tools, knowledge and experience to be able to meet the information security requirements
		4.3	• Allocate responsibility for information security to match business roles	User rights are allocated according to the least privileges principles
				Performance reviews assess against information security objectives expected of the employee
				Acceptable usage and user responsibility policy is documented and enforced
				Information on security issues are made available for users – home user security is supported where access from home is granted.
				E-training and practical exercises for information security are provided for employees and contracts
		4.4	• Define information	Roles and responsibilities for management of external parties is assigned and managed

			security responsibilities for external parties in the engagement contract	External party responsibilities are detailed in service level agreements with requirements such as: • The level of security at external parties is equivalent to that of the organisation itself; • An agreed set of security standards and policies is in place between the parties; • Co-ordination of information security activities such as audits and incident response; and • The allocation of costs associated with remedying information security deficiencies is agreed prior to their occurrence.
5	Information Security Must Consider Internal and External Stakeholders	5.1	• Implement information security controls to support service continuity	The level of business criticality of information infrastructure is assessed
				Service Level Agreements ensuring availability is in place with key partners or suppliers
				Incident response procedure are developed and validated with exercises
				Enterprise business continuity management programmes are structured and implemented
				Business continuity and disaster recovery plans are tested with the aid of dependent and supplier organisations
				Customers are informed of service outages and assistance is provided for their contingency planning
		5.2	• Ensure sensitive customer and community data is protected appropriately	Legal and regulatory obligations for protecting customer information are understood, documented and followed by the organisation.
				Access to customer information is protected by strong access controls, and both 'view' and 'modify' access is logged by the system
				Customers are provided education and awareness materials to help them protect their authentication credentials appropriately

				Service providers (e.g. backup, storage) provide a level of information security equivalent to that of the organisation
				Policy exists on the protection of customer information
		5.3	• Ensure the security of all organisations involved in the business value chain	Provides assistance to connected organisations in achieving a level of required information security
				Joint risk assessments and security exercises are conducted with value chain members
				Security information sharing arrangements with suppliers and customers are in place
				Suppliers and customers roles are defined in the incident response procedure
		5.4	• Consider employee interests in the design of security systems	Employee personal details such as payroll, addresses, dependents, employment history are protected
				Employee communications including email, telephone and mail correspondence are protected
				Employees are involved in system design where decisions may materially affect their needs
				Employees are encouraged to raise ad-hoc concerns regarding information security
				Internal processes are in place for early identification of malicious insiders
6	Information Security Requires Understanding and Commitment	6.1	• Develop and maintain the information security policy to be practical and current	Policy statements are reviewed annually
				Policy statements are clear and concise
				Policy exemption procedure is established
				Business partners provide statement of compliance to the security policy
		6.2	• Establish employee and	Awareness program communicates the importance and relevance of information security to the organisation

			contractor education and awareness programmes relevant to the organisation and individual roles	Awareness program provides 'real world' examples or demonstrations of information security risk scenarios
				Mechanisms to update staff awareness of current security threats
				Clear guidance is provided on how to incorporate security into day-to-day tasks
				An avenue to address staff concerns is provided regarding the impact of information security on their role and the operation of the business
		6.3	• Incorporate information security into existing communications processes	Information security communications are incorporated in existing processes such as: • Change management form • Incident reporting form • News bulletin email templates • Database of emails for key organisational contact points • Helpdesk hotline • Pagers for security staff
				Help desk facilities are provided for staff requiring an avenue to discuss information security concerns
				External communications to investors, regulators and customers are planned and structured
		6.4	• Participate in ad-hoc and formalised information sharing networks	Organisation participates in information sharing through: • Industry organisations • Public/private associations and forums • Critical service or product suppliers • Customers

7	Information Security Requires Continual Improvement	7.1	• Ensure information security expertise and experience is available to meet the organisation's needs	Job description of technical roles incorporate information security responsibilities
				Changes in business strategy are communicated to technical staff in order to define potential security implications
				Resources are allocated to allow technical staff to attend conferences, subscribe to forums and industry associations, as well as conduct internal information sharing for information security
				Service providers are vetted through background and reference checks
				Non-disclosure agreements cover all external provided services
				All communications with external service providers are secured in accordance with the organisation's security policy
		7.2	• Review information security controls against national and international standards	Technical audits of information security are performed to verify known vulnerabilities are not present and risks continue to be mitigated to acceptable levels
				Periodic risk assessments are conducted to validate existing mitigation practices, and assess the impact of changes in the organisation or system's risk profile or external threat environment
				Review duration is determined by • Legal and regulatory requirements • Cost of conducting the review • Changes in the external environment
		7.3	• Implement systems and processes to identify and respond to	User access and rights modification are logged with a focus on privileged and administrative access levels
				Intrusion detection or prevention systems, or system integrity verification software, is implemented to alert system managers of unauthorised access or usage

			malicious or unintended information security breaches	Trained personnel are available to complete investigations if unauthorised access or usage is suspected
				Effective incident escalation procedures are implemented to enable immediate response
		7.4	• Develop a feedback process to incorporate incident details into risk assessments and control selection as part of the systems lifecycle	Post incident meetings are conducted involving incident handling personnel, information security, system and business owners to discuss the speed with which the incident was identified, the response determined and implemented, and the effectiveness of the response
				“Post Incident Reports” are compiled and archived, capturing incident and response details. The report is to be circulated to a controlling group for considering appropriate procedural or policy level changes arising
				New system development acknowledges relevant past incident information and applies recommendations within the design process
				Incident reports are used as input for information security policy, standards and procedure review sessions
		7.5	• Include security as a selection criteria for assessing new technologies for the organisation	Security is considered at the conception and design stage of new technology adoption processes
				Trusted and open standards are used as guidelines for design and management of new technology adoption processes
				Formal documentation of the security requirements for new technology adoption is enforced. Security requirements are listed as an element of “Request For Proposal” (RFP) documents for response from vendors

References

AusCERT, *Computer Crime and Security Survey*, 2006, *http://www.auscert.org.au/images/ACCSS2006.pdf*

Computer Security Institute, *CSI/FBI Computer Crime and Security Survey*, 2006, *http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf*

S Grose, *'Federal Government to Toughen Information Security', ZDNet Australia*, 2006, *http://www.zdnet.com.au/news/security/soa/Federal-government-to-toughen-information-security/0,130061744,139249593,00.htm*

G Wang 'Strategies and Influence for Information Security', Information System Control Journal, vol 1, 2005, Information Systems Audit and Control Association

ITSEAG (Trusted Information Sharing Network), *Leading Practices and Guidelines for Enterprise Security Governance*, 2006, *http://www.dcita.gov.au/__data/assets/pdf_file/41308/IT_Security__and__Governance.pdf*

L Friedman & H Gyr, 'Business Strategy Tools for OD Practitioners: Creating the Dynamic Enterprise, Vision/Action Journal of the Bay Area OD Network', 1998

The Open Group, TOGAF (The Open Group Architecture Framework) Enterprise Edition, Version 8.1, 2003, *http://www.opengroup.org/architecture/togaf8-doc/arch/*

The Open Group, Guide to Security Architecture in TOGAF Architecture Development Method (ADM), 2005, *http://www.opengroup.org/architecture/togaf8-doc/arch/chap03.html*

Attorney-General's Department, Trusted Information Sharing Network: About Critical Infrastructure, 2006, *http://www.tisn.gov.au/*

Trusted Information Sharing Network, *Denial of Service / Distributed Denial of Service – Managing DoS Attacks*, 2006, *http://www.dcita.gov.au/__data/assets/pdf_file/41312/DoS_Report.pdf*

UM Stroh, *An Experimental Study of Organisational Change and Communication Management*, 2005, Faculty of Economics and Management Sciences, University of Pretoria

DL Pipkin, Information Security—Protecting the Global Enterprise, 2000, HP Professional Series

The Zachman Institute for Framework Advancement, *Zachman Framework Definition*, 2007, *http://www.zifa.com/quickstart.html*

The United States Department of Defense, *Enterprise Architecture*, 2007, *http://www.defenselink.mil/cio-nii/cio/earch.shtml*

MSDN, *Service Oriented Architecture*, 2007, *http://msdn2.microsoft.com/en-us/architecture/aa948857.aspx*

Verisign, Building a Security Framework for Delivery of Next Generation Network Services, 2005, *http://www.verisign.com/static/035478.pdf*

Australian National Audit Office, *IT Security Management Audit Report No.23 2005-2006*, 2005, *http://www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf*

The United States National Institute of Standards and Technology, *Information Security Handbook: A Guide for Managers sp800-100*, 2006, *http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf*

OECD, Guidelines for the Security of Information, 2002, *http://www.oecd.org/dataoecd/16/22/15582260.pdf*

The United States National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 1996, *http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf*

Information Systems Security Association, Generally Accepted Information Security Principles, 2003

ISO, ISO/IEC 27001 – Information Technology – Security Techniques – Information Security Management Systems – Requirements, 2006, Standards Australia/Standards New Zealand

Defence Signals Directorate, ACSI 33 Australian Government Information and Communications Technology Security Manual, 2006, *http://www.dsd.gov.au/library/infosec/acsi33.html*

ITIL & IT Service Management Zone, *What is ITIL*, 2002, *http://www.itil.org.uk/what.htm*

IT Governance Institute, *COBIT(3rd Edition) Executive Summary*, 2000, Information Systems Audit and Control Foundation

C Cochran, 'Using Quality Objectives to Drive Strategic Performance Improvement', Quality Digest Magazine, 2000

United States of America, *Sarbanes Oxley Act of 2002*, 2007, *http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf*

W Sonnenreich, J Albanese, & B Stout, 'Return on Security Investment (ROSI): A Practical Quantitative Model', Journal of Research and Practice in Information Technology, vol. 38, no. 1, 2005, *http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT38/JRPIT38.1.45.pdf*

@Stake 2002 as cited in J Reavis, *"CSO White Paper Series - Managing Risk and Reducing the Cost of Web Application Security", CSO Informer,* SPI Dynamics, 2004, *http://www.securitytechnet.com/resource/security/application/SPI-risk-cost-draft-ver2.0.pdf*

S/Keysource.com, *Security Through Obscurity*, 2007, *http://www.skeysource.com/one-time-password/security-through-obscurity.html*

Common Criteria Portal, 2007, *http://www.commoncriteriaportal.org/*

The United States National Security Agency, *Defense in Depth*, 2007, *http://www.nsa.gov/snac/support/defenseindepth.pdf*

SE Harrington & GR Niehaus, *Risk Management and Insurance*, McGraw Hill – Irwin, 2004

National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 1996, *http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf*

Commonwealth of Australia, *Corporations Act 2001, section 180 subsection 1*, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s180.html*

Commonwealth of Australia, *Corporations Act 2001, section 182 subsection 1*, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/s182.html*

JH Saltzer & MD Schroeder, 'The Protection of Information in Computer Systems', The Fourth ACM Symposium on Operating System Principles, 1973, *http://www.cs.virginia.edu/~evans/cs551/saltzer/*

RA Botha & JHP Eloff, 'Separation of Duties for Access Control Enforcement in Workflow Environments', IBM Systems Journal, vol 40, no 3, 2001, *http://www.research.ibm.com/journal/sj/403/botha.pdf*

Trusted Information Sharing Network, Managing IT Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure, 2007, *http://www.tisn.gov.au*

OECD, OECD Principles of Corporate Governance, 2002, *http://www.oecd.org/dataoecd/32/18/31557724.pdf*

Commonwealth of Australia, Trade Practices Act 1974, section 52, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/tpa1974149/s52.html*

Commonwealth of Australia, Corporations Act 2001, 2006, *http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/*

Commonwealth of Australia, National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000, 2007, *http://www.privacy.gov.au/publications/npps01.html*

Australian Securities Exchange, Listing Rules Chapter 3 - Continuous Disclosure, 2003, *http://www.asx.com.au/ListingRules/chapters/Chapter03.pdf*

Trusted Information Sharing Network, Infrastructure Information in the Public Domain, 2006, *http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(4341200FE1255EFC59DB7A1770C1D0A5)~infrastructure-information+in+the+public+domain.23-11-06.pdf/$file/infrastructure-information+in+the+public+domain.23-11-06.pdf*

Network Working Group, Request For Comments (RFC) 2828 Internet Security Glossary, 2000, *http://www.faqs.org/rfcs/rfc2828.html*

The United States Department of Defense, Directive 8570.1 – Information Assurance Training, Certification, and Workforce Management, 2004, *www.amc.army.mil/amc/ci/matrix/downloads/DoD8570.1_MIATCWFM07-29-25.doc*

Asia-Pacific Economic Cooperation, Information Security Skills Certification Guide, 2007, *http://siftsecurity.net/*

Adapted from Gerloff 1984 as cited in Nelson and Quick, Organizational Behavior 5th Edition, South-Western College, 2005