Trusted Information Sharing Network
for Critical Infrastructure Protection

Defence in depth

June 2008

FOREWORD

In today's business environment, controlling access to information is critical to long-term competitive advantage. Alongside significant benefits, every new technology introduces new challenges for the protection of this information. 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 that need to be protected.

This report has been developed by the IT Security Expert Advisory Group (ITSEAG) which is part of the Trusted Information Sharing Network (TISN)[1] for critical infrastructure protection.

TISN has previously released a number of papers to assist CEOs and CIOs in understanding IT security threats and strategic approaches to securing their IT infrastructure. Issues covered in these documents range from managing denial of service risks to information security strategy and governance. These papers are available at: www.tisn.gov.au.

This paper is closely related to the *Secure Your Information* report of June 2007, which was developed to provide strategic guidance for the implementation of information security through seven core principles. The principles reflect the holistic approach required for the management of information security, by consideration for organisational mission, risk factors, internal and external stakeholders and continual improvement.

This paper seeks to develop a practical approach for developing enterprise information security through a layered defence in depth approach with particular reference to the principles and recommendations contained in the *Secure Your Information* report.

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.

[1] TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of nine sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAG), and the Critical Infrastructure Advisory Council (CIAC - which is the peak body of TISN and oversees the IAAGs and the EAGs). More information on TISN can be sought from www.tisn.gov.au or by contacting cip@ag.gov.au. The ITSEAG is one of the expert advisory groups within the TISN framework. The ITSEAG provides advice to the CIAC and the sector-based IAAGs on IT security issues as they relate to critical infrastructure protection. It is made up of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security field. The ITSEAG Secretariat can be contacted on (02) 6271 7018.

Contents

Foreword **2**
Figures 4
Tables 5
Focus area summaries 5
Executive summary **6**
Overview ..... Error! Bookmark not defined.
Critical infrastructure 9
The defence in depth concept 10
Establish context **11**
Enterprise strategy 13
Internal environment 14
Governance 16
People 16
Process 17
Technology 19
Threat environment 21
Adversaries and motivations 21
Risk analysis **23**
Risk profiling 23
Risks, threats and vulnerabilities 23
Risk Analysis methodology 24
Identify risk 25
Analyse risk 28
Evaluate risk 31
Key success factors 32
Assessment methodologies and tools 33
Assessing governance risks 33
Assessing people risks 35
Assessing process risks 38
Assessing technology risks 40
Implementing defence in depth **44**
Core principles 45
Implement measures according to business risks 45
Implement controls using a layered approach 45
Controls should serve to increase the cost of an attack 46
Implement technical, procedural and operational controls 47
Implementing governance controls 47
Accountability 48
Policy and compliance management 48
Control analysis 49
Implementing people controls 56
Job and role definition 56
Recruitment and selection 57
Induction, training and development 58

Ongoing operations 59
Role change management 59
Managing morale 59
Termination of employment 59
Control analysis 60
Implementing process controls 63
Protect 63
Detect 64
React 64
Control analysis 65
Implementing technology controls 74
Information-centric technical controls 74
Multi-use technical controls 75
Application (client and server) 75
Host (client and server) 76
Network 78
Control analysis 78
Monitor and review 88
Strategies for managing change 88
Governance 89
People 89
Process 90
Technology 90
Emerging challenges 91
Governance risks 91
People risks 92
Process risks 93
Technology risks 94
Appendices 96
Appendix A: Glossary 96
References 97

Figures

Figure 1: Defence in depth life cycle 9
Figure 2: Critical infrastructure industries 10
Figure 3: Applicable principles of information security for establishing the risk context 12
Figure 4: Enterprise strategy structure 13
Figure 5: People, process, technology and governance—potential weaknesses 16
Figure 6: Layer of protection analysis (LOPA)—control layers 19
Figure 7: Information sensitivity and system criticality matrix 20
Figure 8: Layered technical security controls 21
Figure 9: Applicable principles of information security for analysing the risk context 24
Figure 10: Risk assessment project approaches 26
Figure 11: MECE risk-analysis tree 27
Figure 12: Inductive and deductive threat analysis models 28
Figure 13: Relationship between objectives, strategies and process. 39

Figure 14: Applicable principles of information security for implementing defence in depth . 45
Figure 15: Layer of protection analysis (LOPA)—control layers 47
Figure 16: Top-down definition of framework, policy and procedures..... 50
Figure 17: Protect, detect, react, revise model..... 64
Figure 18: Sample technology information flow..... 75
Figure 19: Applicable principles of information security for monitor and review..... 89

Tables

Table 1: External service providers and outsourcers..... 18
Table 2: AS4360 risk rating levels..... 33
Table 3: Sample governance vulnerabilities and classification..... 35
Table 4: Sample governance threats and classification 35
Table 5: Sample people vulnerabilities and classification..... 38
Table 6: Sample people threats and classification..... 38
Table 7: Sample process vulnerabilities and classification..... 40
Table 8: Sample process threats and classification..... 40
Table 9: Sample technology vulnerabilities and classification..... 43
Table 10: Sample technology threats and classification..... 43

Focus area summaries

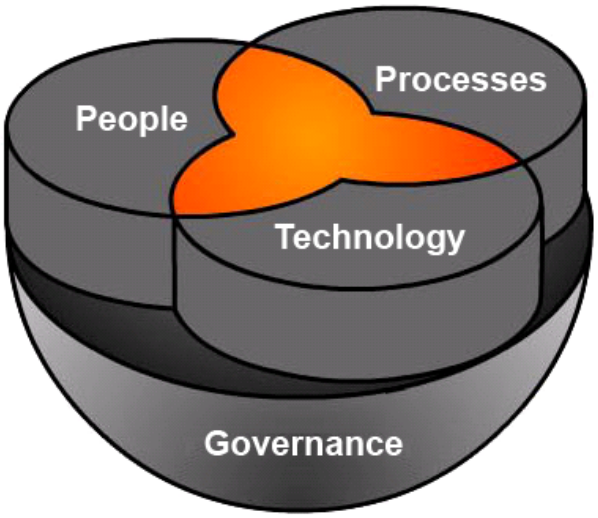
Focus area guideline 1: Risk management..... 51
Focus area guideline 2: Policy and compliance management 53
Focus area guideline 3: Information security..... 55
Focus area guideline 4: Personnel security..... 62
Focus area guideline 5: Incident response management..... 67
Focus area guideline 6: Audit management..... 69
Focus area guideline 7: User-access management..... 71
Focus area guideline 8: Identity management 73
Focus area guideline 9: Infrastructure security..... 80
Focus area guideline 10: Communications security 83
Focus area guideline 11: Network architecture security..... 85
Focus area guideline 12: Application security..... 87

EXECUTIVE SUMMARY

For critical infrastructure organisations today, a consistent and reliable approach to information security is essential. As organisations become increasingly interconnected, the need to examine the environment to identify weak points—whether in people, processes, technology or governance—has never been more important.

Defence in depth is the intelligent security management of people, processes and technology, in a holistic risk-management approach. It is based on military strategy which says that defences are primarily in place to delay rather than prevent the advance of an attacker. In the military context, this relies on the assumption that an attack will lose momentum over a period of time, and time will allow those being attacked to respond appropriately.

In an IT environment, defence in depth is similarly intended to increase the cost and effort of an attack against the organisation, by detecting attacks, allowing time to respond to such attacks, and providing layers of defence such that even a successful attack will not fully compromise an organisation.



People
Security roles & responsibilities for internal and external persons

Process
Standardised actions which are used to ensure security posture is sustained

Technology
Solutions employed which enable the achievement of business objectives

Governance
Management framework providing oversight and coordination of people, process and technology

Critical infrastructure organisations should recognise the need to provide coordinated and multi-layered security architectures to mitigate information security risks. Furthermore, security should not rely solely on point solutions as a single control failure may result in a complete compromise. Implementing defence in depth requires an understanding of enterprise strategy—including the organisation's overarching goals and business environment—as well as their physical, information and intangible assets, and the internal and external threat environment.

Although technology provides some of the controls used in defence in depth, it is far more than an IT concept, as it provides for:

- **supporting effective risk-based decisions to be made**—ensuring consistency with the organisation's broader risk management framework

- **enhancing the organisation's operational effectiveness**—through effectively allocating resources and addressing priority issues
- **reducing overall cost and risk associated with information security**—through minimising investment that is not aligned with genuine risk mitigation and loss prevention.

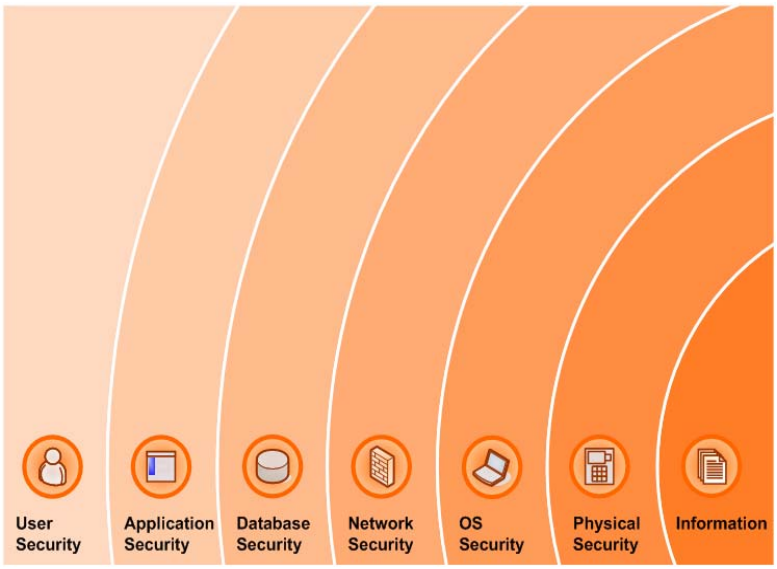
A defence in depth strategy has become increasingly important as a direct result of overall business and IT trends that have led to weakened organisational controls of critical information assets, including:

- break down of the perimeter
- mobile workforce
- decentralisation of services
- increasing value of information.

A fundamental principle in defence in depth is the balanced and coordinated approach across people, process (operations) and technology[2]. An overriding element of governance responsibility is also required to manage the coordination of these elements.

The core principles of a defence in depth strategy are:

1. **Implement measures according to business risks.**
2. **Use a layered approach—as illustrated at right—such that the failure of a single control will not result in a full system compromise**.
3. **Implement controls such that they serve to increase the cost of an attack.**
4. **Implement personnel, procedural and technical controls.**



Additionally, defence in depth requires that mechanisms be implemented to protect against attack, to detect such attacks and to provide an effective response.

In order to successfully implement defence in depth in an organisation, management must include these core principles within the organisation's strategy, planning and structure. These core principles then correspond to design and implementation actions in the areas of governance, people, process and technology.

The high-level principles as identified in the *Secure Your Information* report will then flow through into such actions as:

[2] US NSA, *Defense in Depth*, www.nsa.gov/snac/support/defenseindepth.pdf

- coordinating and ensuring alignment of physical, personnel and IT security programs
- enforcing separation of duties
- implementing relevant and targeted procedural, operational and technical controls
- developing and implementing redundancy and contingency plans as part of the business continuity program
- assessing the impact and risk of control failure and ensuring that secondary controls are in place to address such an event.

This report works through the defence in depth life cycle, from:

- establishing the risk context of the organisation
- completing a risk analysis
- implementing defence in depth controls
- monitoring and reviewing the application of the defence in depth strategy to ensure its effectiveness.

In implementing defence in depth controls, specific attention is provided to key focus areas, as defined by the Australian Government Attorney-General's Department, as follows:

Governance

- Risk management.
- Information security.
- Policy and compliance management.

People

- Personnel security (including user awareness).

Process

- User-access management.
- Identity management.
- Incident response management.
- Audit management.

Technology

- Communications management.
- Infrastructure management.
- Network architecture management.
- Application security.

While new threats are arising constantly, the strategy of defence in depth has proved its value over hundreds of years. The use of the core principles described in this report, in conjunction with risk management, will ensure an appropriate and effective information security profile is maintained.

OVERVIEW

The overview section of this paper provides an introduction to defence in depth in the context of Australia's critical infrastructure organisations. Existing literature on the topic of defence in depth from Australia and overseas was reviewed and appraised, to ascertain best-practice recommendations for implementation of defence in depth.

The report is divided into four main sections, following a life cycle model for strategic implementation (see Figure 1). These are:

- **Establishing context**—provides context for the necessary inputs into the development of a robust defence in depth framework.
- **Risk analysis—**provides a methodology and key considerations for assessing the organisation's current state of defences.
- **Implement defence in depth—**provides a framework for implementing a holistic set of defence in depth controls across governance, people, process and technology.
- **Monitor and review—**provides considerations to ensure ongoing relevance of the defence in depth framework.

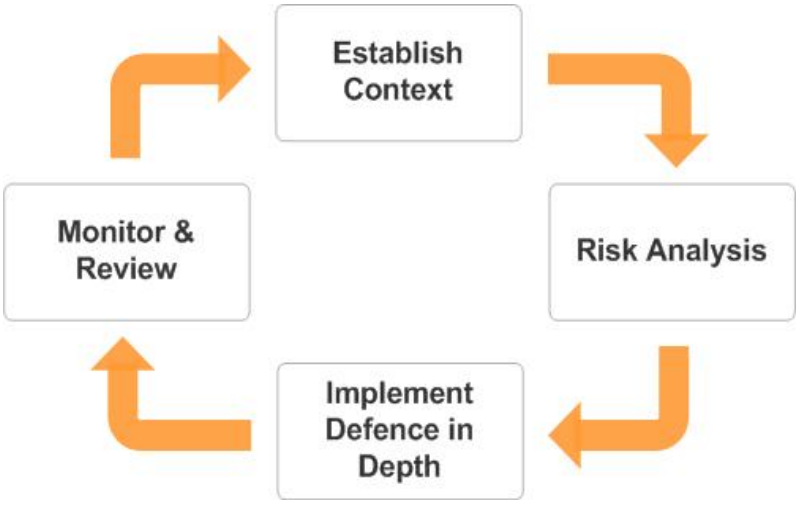


Figure 1: Defence in depth life cycle

Critical infrastructure

The Australian Government Attorney-General's Department 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*[3].

[3] TISN, *About Critical Infrastructure*, 2006, www.tisn.gov.au

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

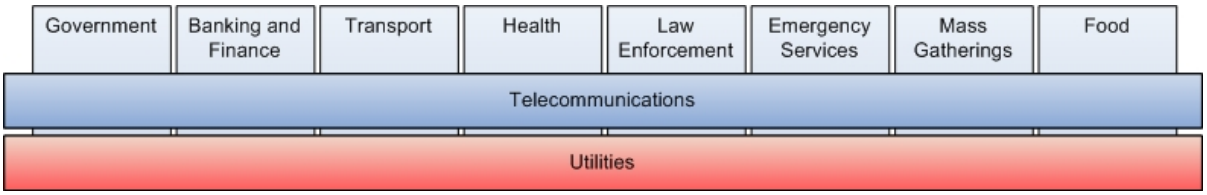


Figure 2: Critical infrastructure industries

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[4] 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 then 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 per cent of critical infrastructure in some Australian areas is in private hands[5].

The nature of critical infrastructure is such that it encompasses regulators, private sector and public sector, providing a significant challenge for development of policy and governance. Due to the interconnected nature of critical infrastructure, a holistic approach to defining defence strategies is required, as is provided by defence in depth.

The defence in depth concept

Defence in depth is a military strategy with foundations in early human history[6], with a core belief being that defences are primarily in place to delay rather than prevent the advance of an attacker. In the military sense, this relies on the assumption that an attack will lose momentum over a period of time, and time will allow those being attacked to respond appropriately.

Many non-military applications of the defence in depth principles now exist, including both physical and logical protections for mission critical or potentially hazardous sites such as nuclear power stations or chemical engineering plants. In the context of computing, defence in depth is an approach conceived by the US National Security Agency (NSA) as a comprehensive approach to information and electronic security.

The core concept of defence in depth is to use multiple defence mechanisms in layers across the enterprise architecture, across IT and non-IT components, with the objective of securing

---

[4] TISN, *Denial of Service/Distributed Denial of Service – Managing DoS Attacks*, 2006, http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications

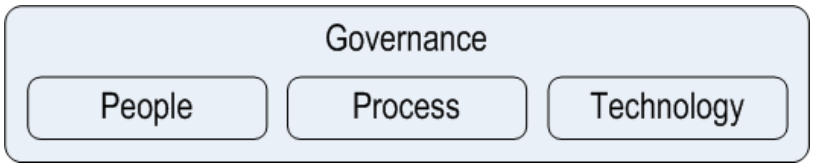
[5] Grose S, *Federal Government to Toughen Information Security*, *ZDNet Australia*, 2006, www.zdnet.com.au/news/security/soa/Federal-government-to-toughen-information-security/0,130061744,139249593,00.htm

[6] Parker G, *The Military Revolution: Military Innovation and the Rise of the West 1500-1800*, Cambridge University Press 1996.

internal information, systems, networks and users[7]. As the strength of any system is no greater than its weakest link, the defence in depth strategy ensures that should one defensive measure fail there are other defensive measures in place that will continue to provide protection[8].

A fundamental principle in defence in depth is the balanced and coordinated approach across people, process (operations) and technology. An overriding element of governance responsibility is required to manage this coordinated effort. These elements are described in detail as follows:

- **Governance** —the governance element of defence in depth refers to the overriding management framework used to provide oversight and coordination of people, process and technology elements.
- **People**—the people component of defence in depth describes the definition, maintenance and enforcement of security roles and responsibilities for both internal and external employees and vendors.
- **Process**—the process component of defence in depth describes the definition, maintenance and enforcement of standardised actions which are used to develop and ensure that security posture is sustained on a day-to-day basis.
- **Technology**—the technology component of defence in depth describes technology and product solutions that are employed to enable the achievement of business objectives in a sustainable manner.



While not specifically providing requirements to approach security from a defence in depth perspective, security standards such as ISO 27002 and the Payment Card Industry Data Security Standard (PCI DSS) outline many of the same underlying principles and provide an approach to security consistent with defence in depth. The *Australian Government Information and Communications Technology Security Manual* (ACSI 33) recommends a defence in depth approach to physical security[9].

ESTABLISH CONTEXT

The information security principles from the *Secure Your Information: Secure Your Business* paper relevant to this section are:

[7] Straub KR, *Information Security: Managing Risk with Defence in Depth*, August 2003, www.sans.org/reading_room/whitepapers/infosec/1224.php
[8] Northcutt S, *Information Centric Approach to Defense in Depth*, February 2007, www.sans.edu/resources/securitylab/321.php
[9] Australian Government, *Australian Government Information and Communications Technology Security Manual (ACSI 33)*, September 2007, www.dsd.gov.au/library/infosec/acsi33.html

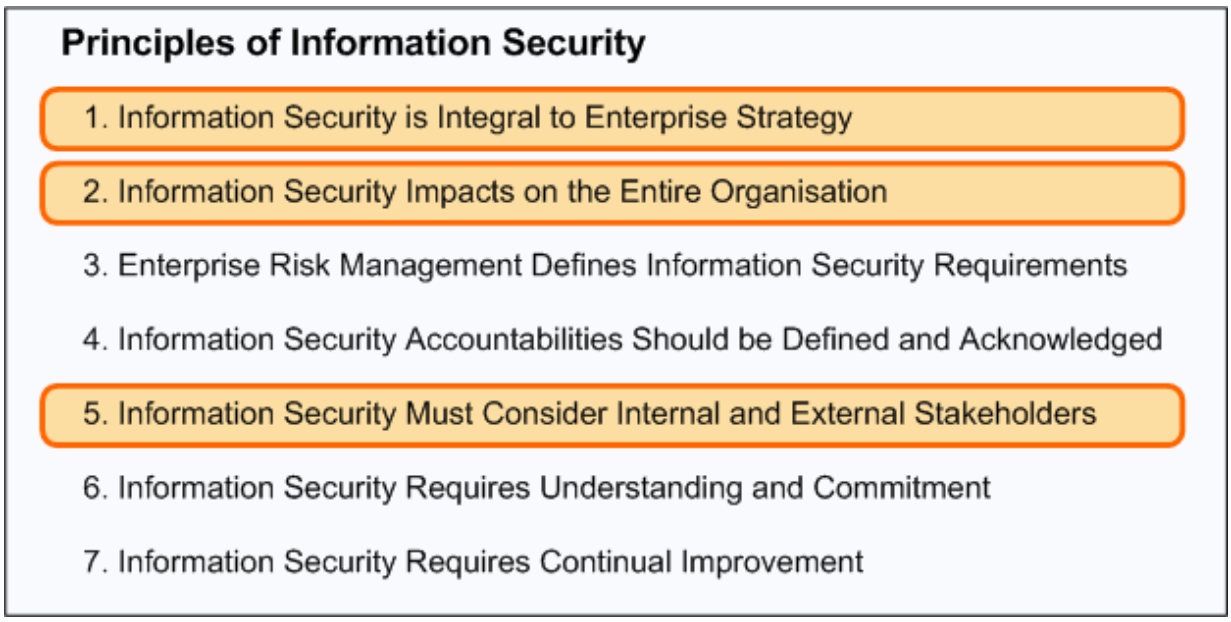


Figure 3: Applicable principles of information security for establishing the risk context

As stated within AS 4360 *Risk Management Standard*, 'the major risk for most organisations is that they fail to achieve their strategic, business or project objectives, or at least perceived to have failed by various stakeholders.'[10] Many strategies, businesses and projects rely on the confidentiality, integrity and availability of information and, in this context, a defence in depth strategy is essential for ensuring that this key risk is addressed.

According to the Information Security Forum, the main characteristics of an effective risk-analysis capability are that it is:

- business-driven
- placed at the centre of an overall information risk-management approach
- widely deployed.[11]

In order to effectively deploy such a capability—and a corresponding defence in depth strategy—it is therefore necessary to have accurate and relevant organisational and environmental intelligence, coupled with effective ongoing internal reporting and communications.

This section of the report discusses the three main components necessary for analysis in order to allow an organisation to effectively establish the risk context within which the defence in depth strategy is to be implemented:

- enterprise strategy
- internal environment, assets and systems
- threat environment.

[10] Standards Australia, *AS 4360: Risk Management Standard*, 2004.
[11] Information Security Forum, *Business Impact Analysis*, June 2004, www.securityforum.org/assests/pdf/iram_assort.pdf

Enterprise strategy

The intent of defence in depth is to provide an appropriate level of controls in order to balance the risk of loss with the cost of control, and support the provision of the fundamental services that the organisation is in place to deliver. To achieve this, it is necessary for the organisation to have an understanding of its core mission and goals as these will ultimately dictate what is of value to the organisation and hence what has the greatest need for protection.

An effective enterprise strategy allows an organisation to create a unique and valuable market position. In order to understand the scope of enterprise strategy, it is important to consider the layers of strategy within an organisation[12].

- **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 into specific short to medium-term objectives that 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

Using the enterprise strategy structure of Figure 4, it is important to note that while defence in depth strategy is planned and driven from the top down, the operational implementation and communication of the strategy will generally occur bottom up, with consultation of existing business processes, stakeholders and resources. It is this structural delineation that creates significant importance around the 'people' element of the people, process and technology triad.

A defence in depth strategy has become of increasing importance as a result of overall business and IT trends which may weaken organisational control of information assets, including[13,14]:

---

[12] TISN, *Secure Your Information*, April 2007, www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~SIFT_Full_Report+020707.pdf/$file/SIFT_Full_Report+020707.pdf

[13] Pipkin DL, *Information Security—Protecting the Global Enterprise,* 2000, HP Professional Series.

[14] Brooke P, *Building an In-Depth Defense*, Network Computing, 2001, www.networkcomputing.com/1214/1214ws1.html

- **Break down of the perimeter**—the trend towards organisations having a hard-to-define external boundary, resulting from the creation of close relationships with customers, business partners, staff, suppliers and the use of increased mobility.
- **Mobile workforce**—employees are increasingly required to work in non-conventional environments with flexible arrangements and requiring flexible access to information and systems.
- **Decentralisation of services**—the provision of services and systems that were previously available only to a tightly controlled internal group of users, to a broader set of users via the internet and extranets.
- **Increasing value of information—**the significance of information in building a sustainable competitive advantage has rapidly increased. As Grace Hopper put it, 'some day, on the corporate balance sheet, there will be an entry which reads, "Information"; for in most cases, the information is more valuable than the hardware which processes it.'[15]

Given these trends, it has become critical for organisations to accurately assess and position their risk exposure, and to have a dynamic awareness of the key information and assets subject to protection by the organisation. This corresponds to the 'Develop risk criteria' phase of the AS 4360 *Risk Management Standard*. As noted in this standard, this requires an organisation to define the criteria against which risks are to be evaluated. This can incorporate consideration of:

- **Operational—**the degree to which a risk may interrupt the ability of the organisation to continue to provide its core services to its constituents.
- **Technical—**identification of key systems and technology components such that an impact to these systems receives the appropriate prioritisation.
- **Financial—**quantifying the organisation's financial thresholds for determining necessary responses to risk items.
- **Legal—**non-compliance with laws and regulations can lead to penalties via the implementation of fines or allocation of damages via a civil court case. In some scenarios criminal penalties for directors may also exist.
- **Brand and media—**the degree to which negative media coverage may arise from a given risk eventuating, and the brand impairment that may ensue.
- **Social—**the impact of a given risk on the broader organisation or local community.
- **Other criteria—**depending on the organisation, other criteria may be relevant for consideration in defining the basis against which a risk will be assessed.

Internal environment

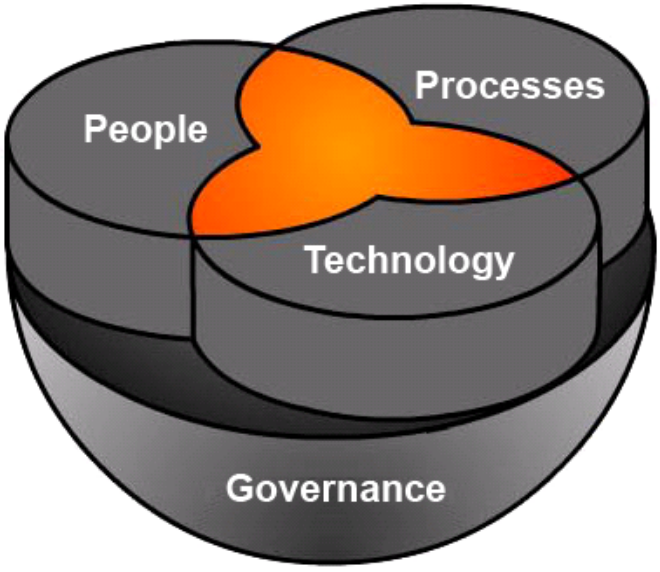
Before considering the business assets and services requiring protection through a defence in depth model, it is necessary to have a comprehensive understanding of the scope of such assets and services. At a high level, assets will include:

[15] Lewis JJ, About.com: *Grace Hopper Quotes*, 2005, http://womenshistory.about.com/od/quotes/a/grace_hopper.htm

- **Physical assets**—tangible and material assets held by the organisation that will generally appear on the organisation's balance sheet. These will include both IT-related physical assets—such as servers and network equipment—and non-IT-related physical assets—such as buildings and facilities.
- **Information assets**—while every organisation creates and uses information daily, specific parts of this information can be reasonably categorised as 'assets' of the organisation. Information assets are hence specifically identifiable and definable pieces of information, stored in any manner, that are considered of value to the organisation[16]. Such information assets could include the organisation's client list, network designs or operating procedures.
- **Intangible assets**—these assets may or may not appear on the balance sheet, however, certain risks or events can have an impact on their value to the organisation. An example is the goodwill associated with an organisation's brand, which can be devalued through a security incident impacting on the reputation associated with the brand.

Defence in depth requires practitioners to place a value on information assets as part of the analysis process. This assessment of business 'value' is necessary to complete meaningful cost-benefit analyses with regards to proposed controls. This value exceeds the nominal accounting value of the asset by inclusion of the benefits the asset generates for the organisation's business. However, the security of physical and intangible assets will also impact upon the security of information asset components.

Consideration of the internal environment mandates the assessment of the organisation's assets and operations throughout the domains of people, process, technology and governance.



People
Security roles & responsibilities for internal and external persons

Process
Standardised actions which are used to ensure security posture is sustained

Technology
Solutions employed which enable the achievement of business objectives

Governance
Management framework providing oversight and coordination of people, process and technology

Figure 5: People, process, technology and governance—potential weaknesses

[16] Stevens J, *Information Asset Profiling*, June 2005, www.sei.cmu.edu/publications/documents/05.reports/05tn021/05tn021.html

Governance

Analysing the enterprise's internal environment involves the consideration of business and governance level issues such as:

- **Business strategy**—the ultimate impact of any risk can only be assessed once the organisation's goals and objectives are clearly understood, as it is the degree to which the goals and objectives are interfered with that is the measure of the business consequence. Similarly, the selection of defence in depth controls will necessarily be consistent with the organisation's goals and objectives if they are to be successfully implemented.
- **Culture**—the OECD *Guidelines for the Security of Information Systems and Networks* issued in July 2002 created the goal of achieving a culture of security[17]. The guidelines constitute a foundation for work towards a culture of security throughout society and are also broadly applicable within an organisation. The culture within an organisation will have a significant influence on the likelihood of given risks occurring, and the degree to which varying control approaches will be successful.
- **Internal stakeholders**—as identified by the information security principle that 'information security impacts on the entire organisation', there can be a large number of internal stakeholders in the area of information security. In order to effectively implement defence in depth, all key stakeholders must be aware of the initiatives and must play their part in supporting the security of the organisation. Management of internal stakeholders requires the inclusion of all staff members in the security program.
- **Organisational structure**—the organisation's structure is important for a number of reasons. Firstly, an awareness of the organisation's structure is necessary to ensure that all key stakeholders have been engaged in any risk identification and analysis project. Secondly, the structure of the organisation will influence the risk exposure of the various organisational components as well as influencing the way in which any selected defence in depth controls would need to be applied.

People

The 'people' element of people, process and technology has been described as a 'force multiplier' of the other elements[18]. The 'force multiplier' concept refers to the fact that the degree to which the people in an organisation effectively design, implement and use processes and technology will ultimately determine the value that is obtained from all other components.

People are a crucial element of any organisation's information security approach. The degree to which the organisation's staff embodies a culture of security will significantly influence that organisation's ability to protect key assets. The OECD culture of security concept comprises nine principles[17]:

- Awareness.
- Responsibility.

[17] OECD, *Guidelines for the Security of Information Systems and Networks*, July 2002.
[18] TeleTech, *Human Capital as a Force Multiplier*, January 2007, www.teletech.com/teletech/file/pdf/White%20Papers/HC_White_Paper.pdf

- Response.
- Ethics.
- Democracy.
- Risk assessment.
- Security design and implementation.
- Security management.
- Reassessment.

In order to identify risks attributable to people, the organisation needs a thorough understanding of internal business structure, personnel classifications, job roles, levels of supervision, and interactions with the external environment. Normal business processes should be interpreted to try to identify types of accidental exposure, along with motivations or opportunities available to mischievous or malicious attackers[19].

In order to establish the context associated with personnel within the organisation, as a component of a defence in depth approach, it is necessary to develop a comprehensive picture of the personnel involved in an organisation. This will include:

- **Employees**—who are likely to be known and centrally coordinated via the human resources (HR) department.
- **Contractors**—who may be known and centrally coordinated via the HR department, or may be engaged and managed directly by individual business units within the organisation.
- **Service providers and outsourcers**—which will include a wide range of organisations and individuals. A list of sample service providers is included in **Table 1**.

Building management	Telecommunication service provider
Electricity provider	Insurance company/broker
Physical security services provider	IT hardware service provider
Data centre provider	IT application provider
Internet service provider (ISP)	Systems backup provider
Other IT service providers	Off-site document/tape storage provider
Banking services provider	Marketing agency

Table 1: External service providers and outsourcers

All of these groups of people will have access to the organisation's information assets and will play a part in the overall security of the organisation’s systems and information.

Process

The ‘process’ component of people, process and technology can be effectively broken down into four key areas[18]:

- Documented methods to govern the operations of the firm.
- Formal training in these methods.
- The degree to which the organisation effectively implements the methods, observes compliance and assesses performance.
- Good procedural design and good adherence to the process.

Processes within an organisation can be analysed through a 'business impact assessment' (BIA)[11], which provides an evaluation of the organisation's business processes to determine their criticality, system and process dependencies and subsequent business impact if not available. Key areas to be considered when analysing business processes include:

- **Business processes—**a business process analysis starts with the identification of the critical processes within the organisation and subsequently assesses key attributes of these processes, such as the maximum acceptable outage, the current protection/recovery capability, the impact on business stakeholders of an interruption, dependent assets and ownership, and alternative processing options.
- **System and process dependencies**—having identified the organisation's processes via a business process analysis, it is necessary to assess the IT system dependencies and requirements of these processes, as well as the inter-relationship between processes. This will allow organisations to accurately identify scenarios in which an impact on a process or system considered of lesser importance could have a flow-on effect on a system of greater importance.
- **Current control structure**—given an understanding of the organisation's critical processes and their inter-relationships, the control structure surrounding the processes requires identification and assessment. Layer of protection analysis[20] is a simplified form of quantitative risk assessment used to identify and assess the protection provided by a set of control layers. These control layers will generally include both technical and process controls. **Figure 6** provides a graphical representation of the potential layers of control implemented around an information asset.

[19] MI5 Security Service Report, *Personnel Security: Managing the Risk – 2nd edition*, accessed 2008: www.cpni.gov.uk/Docs/Managing_the_Risk_2nd_edition.pdf, p14.
[20] EPCONSULT, *Layer of Protection Analysis (LOPA)*, 2005, www.ep-consult.com/hazard_identification.shtml

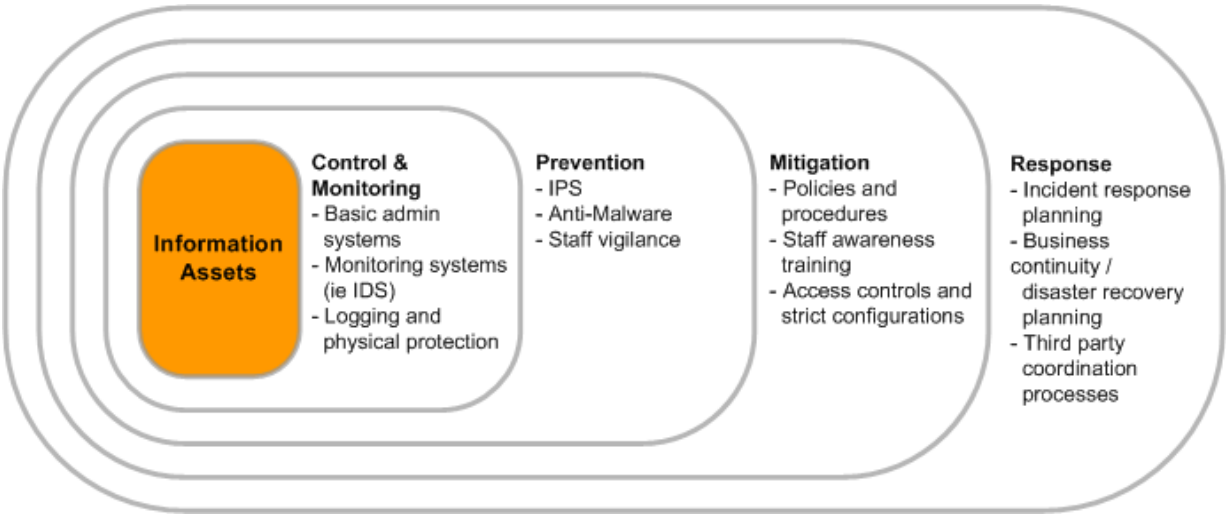


Figure 6: Layer of protection analysis (LOPA)—control layers

Using this model, the individual protection layers—whether currently in place or proposed for implementation—can be analysed for their combined effectiveness, and be considered in the context of the threat environment.

Technology

As per the processes described above for identifying and quantifying the non-technical elements that comprise the organisation's operations, it is similarly necessary to establish the technology context for the organisation.

In order to complete such an analysis, it is first necessary to establish an inventory of all current information systems and technologies within the organisation. Key factors which require understanding in this stage include the:

- extent of the organisational perimeter
- scope of information flows
- architecture of the technology environment
- existence of interconnections and interdependencies.

The criticality of systems is generally determined by the relationship between these information systems and the business processes they support—as identified by the business process analysis discussed in the previous section.

An approach for representing systems by their criticality both to the organisation's overall goals and objectives, and also the information contained within is the matrix shown in **Figure 7**. Each intersecting row and column can be used to capture details about the specific systems within the organisation, their level of data sensitivity and criticality to operations.

Criticality \ Sensitivity	Not Sensitive	Sensitive	Very Sensitive	Highly Sensitive
Not Critical				
Critical				
Highly Critical				

Figure 7: Information sensitivity and system criticality matrix[21]

Technical controls implemented to protect these critical systems can then be assessed in the context of the 'layered' model shown in **Figure 8**, with controls being selected as appropriate for each layer.

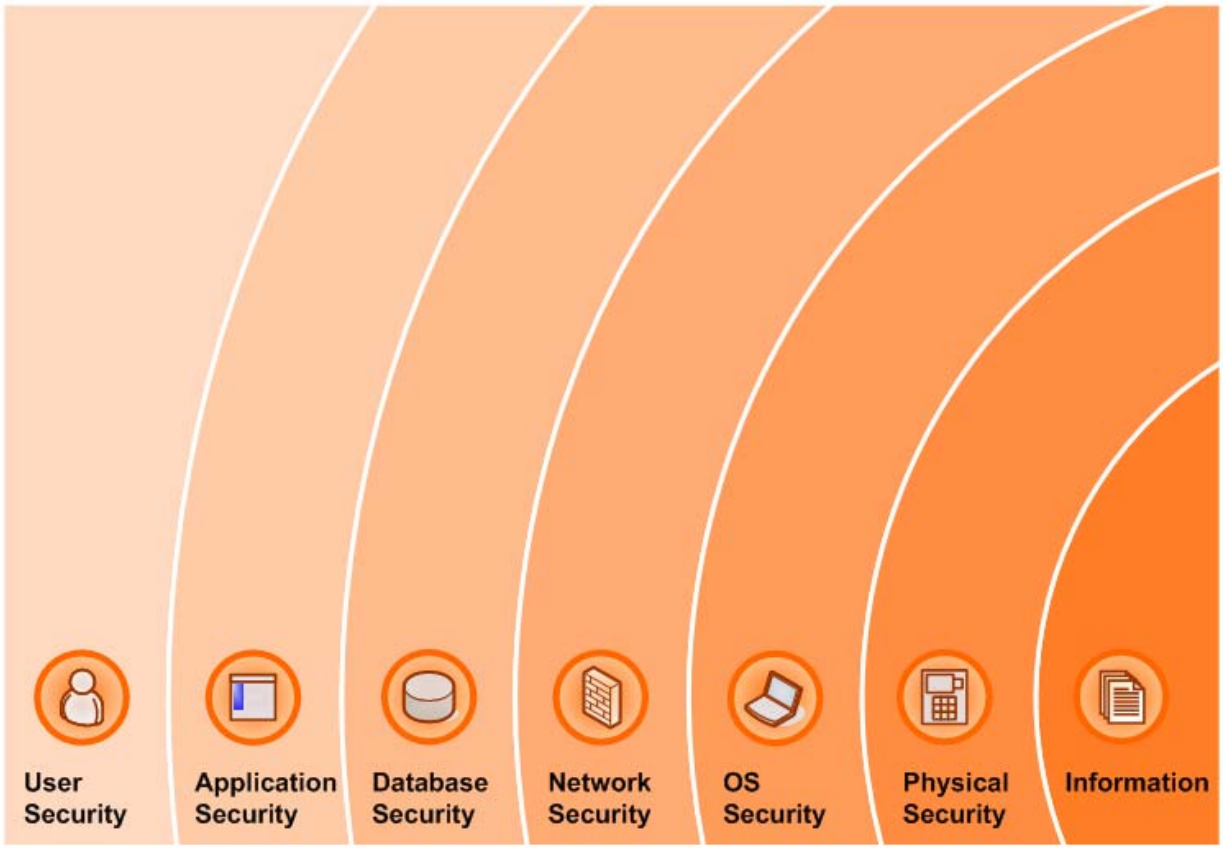


Figure 8: Layered technical security controls

[21] Arkansas Department of Information Systems, *Policies/Standards/Best Practices*, 2005, www.dis.state.ar.us/poli_stan_bestpract/word/data_grid.doc

Threat environment

This corresponds to the 'Establish the external context' phase of AS 4360 *Risk Management Standard*, in which the external environment is examined. Within AS 4360, this is a broad consideration and includes:

- the business, social, regulatory, cultural, competitive, financial and political environment
- the organisation's strengths, weaknesses, opportunities and threats
- external stakeholders
- key business drivers.

For the purposes of considering the requirement for defence in depth, a specific analysis of the threat environment is necessary and inclusion of internal threats is also recommended. Considering potential adversaries and their motivations is the first stage in this process.

Adversaries and motivations

While the specific adversaries for a given organisation will vary based on its market segment, services provided, client base and operations, a base set of potential adversaries can be used to support the assessment. These potential adversaries include:

- **Competitors**—competitors may use information security attack techniques in the interests of industrial or corporate espionage[22], which refers to actions taken by individuals, corporations or governments in the interests of furthering their objectives with regard to a competitor—generally to achieve a financial or competitive advantage through the theft of information or disruption of operations.
- **Criminals**—a significant shift over the past three to five years has been the move towards the coordination of online crime and the increased interest that organised crime has taken as a result. With significant opportunity to obtain financial benefits from both businesses and consumers, criminals have become a significant source of attacks on IT systems.
- **Politically motivated attackers**—politically motivated attacks have the goal of exploiting weaknesses in the security of organisations in order to bring attention to their cause, whatever that may be. In this context, this includes 'hacktivists' as well as malicious attackers that use technology in furthering 'real world' incidents, or engage in purely electronic means of attacks against information, computer systems, computer programs and data.
- **Hackers**—hackers range from 'script kiddies' who download tools and often do not understand the detail of their actions, to more experienced hackers seeking to gain access to a system, and professionals—who cross over into the 'criminals' category—who may hack into a system or organisation on behalf of a third party for payment.
- **Insiders (disgruntled or negligent employees)**—with legitimate access to an organisation's information systems, insiders—whether disgruntled and malicious, or simply careless and negligent—are in a position to cause significant damage to an organisation. Insiders will also include personnel who have worked at or with the

[22] Robinson S, *Corporate Espionage 201*, 2007, www.sans.org/reading_room/whitepapers/engineering/512.php

organisation recently, as well as personnel of contractors and service providers who have worked closely with the organisation and have intimate internal knowledge.

In addition to these adversaries, a risk also exists for indirect damage to occur to an organisation's IT systems as a result of 'collateral damage,' or being used as part of the attacker's infrastructure. The concept of collateral damage refers to such scenarios as sharing IT infrastructure in a hosting service provider with an organisation that is subject to attack, which impacts on your own organisation's service levels. Becoming a part of an attacker's infrastructure generally involves having systems compromised and used by the attacker for further attacks, such as to relay spam or to be a part of a botnet used for denial-of-service attacks.

The motivation for attackers can also vary widely, with some of the more common reasons for attacks being:

- intelligence gathering
- theft of intellectual property
- denial of service
- brand damage
- monetary gain
- revenge
- challenge
- ego.

It is important to consider a given attacker's motivation because it will directly affect the effort and investment that attacker is willing to make in pursuing their objectives. An attacker motivated by monetary gain is unlikely to 'invest' more money in an attack than they would expect to gain from succeeding. However, such 'cost-benefit' analysis may not influence an attacker motivated by revenge or ego.

RISK ANALYSIS

The information security principles from the *Secure Your Information: Secure Your Business* paper relevant to this section are:

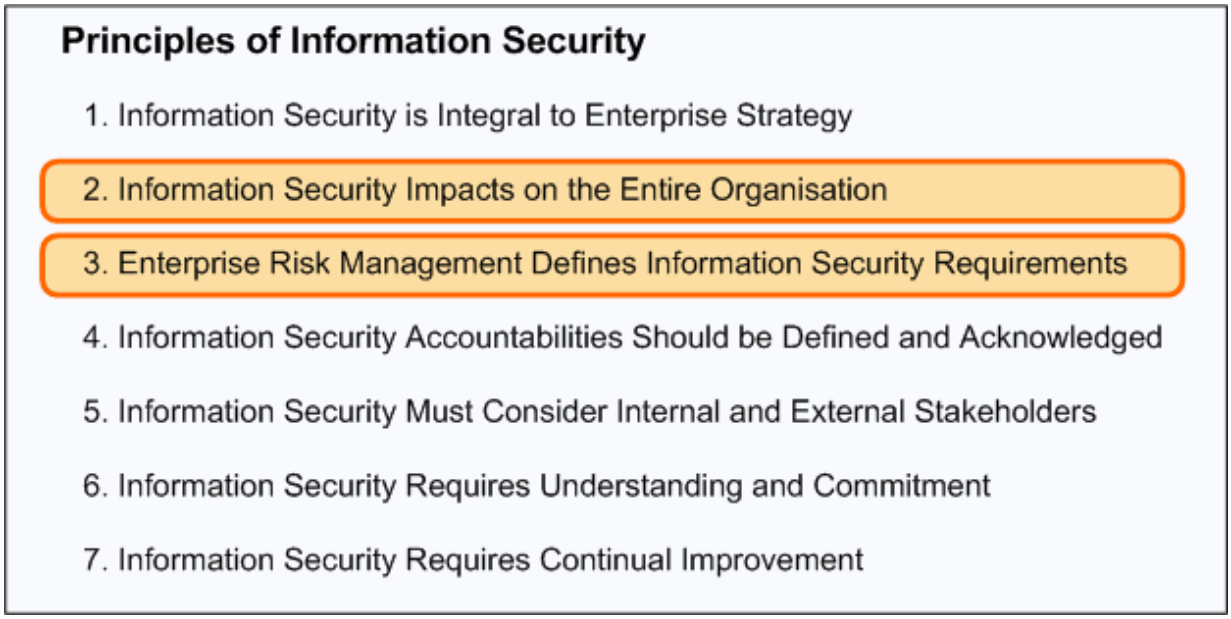


Figure 9: Applicable principles of information security for analysing the risk context

Risk profiling

Understanding and managing the risk profile of an organisation is critical to sustaining competitive advantage. The use of risk assessments to gain the necessary information needed to understand factors negatively influencing business operations and outcomes can allow executives to make informed judgments regarding the extent of actions needed to reduce risk[23]. From a defence in depth perspective, effective risk-analysis outcomes provide the foundations for implementing security controls which are both justified and cost-effective.

While the previous section—*Establish context*—dealt with the external and internal factors influencing an organisation's risk environment, this phase in the defence in depth life cycle is used to determine where the organisation currently stands in terms of the key risk areas.

Risks, threats and vulnerabilities

Information security risks are scenarios through which potential negative impact to an organisation's information assets may occur. Risks are generally a result of an external or internal threat taking advantage of an existing vulnerability within the organisation's governance, people, process or technology infrastructure.

[23] US General Accounting Office, *Information Security Risk Assessment – Practices of Leading Organisations*, November 1999, www.gao.gov/special.pubs/ai00033.pdf

Threats can thus be anything which can negatively affect the confidentiality, integrity, or availability of your systems and/or data. The two common threat types are physical threats (fire, politically motivated attacks, floods, etc.) and electronic threats (viruses, denial of service attacks, hackers, etc.). There are also two sources of threats: external and internal[7].

Vulnerabilities are weaknesses in systems or devices that allow threats to compromise a system. Vulnerabilities will exist in every system. The responsibility of the organisation is to protect the value and operations of the business through the management of these vulnerabilities.

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*[24]

Risk Analysis methodology

The risk-assessment process requires coordination across the organisation. Best practice stipulates that this coordination role should be assigned to an individual or group, depending on the scope of the assessment. A risk analysis will require a number of phases, including[23]:

- **Planning and preparation**—a central coordinator or team is assigned and in conjunction with stakeholders will develop an execution plan. To ensure objectivity, the coordinator should be outside the group assessed. Coordination of interviews and workshops, as well as potential questions, are developed.
- **Conducting the risk assessment**—this is the main information collection and analysis phase. This process may include interviews and workshops with relevant stakeholders to gather past incident information and the presence of existing controls. Threats should be considered in the context of the operational environment. A standardised approach in line with AS 4360 should be followed as best practice.
- **Documentation and reporting—**reporting provides the assessment with concrete remediation strategies and allows for assignment of accountability. Remediation action plans are then developed by the business manager as a result of the findings.

Indicative flowcharts of these project phases are shown in **Figure 9**. These are examples only—the key is to have a standardised approach defined for *your* organisation through analysis of internal requirements, working habits and documentation needs.

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

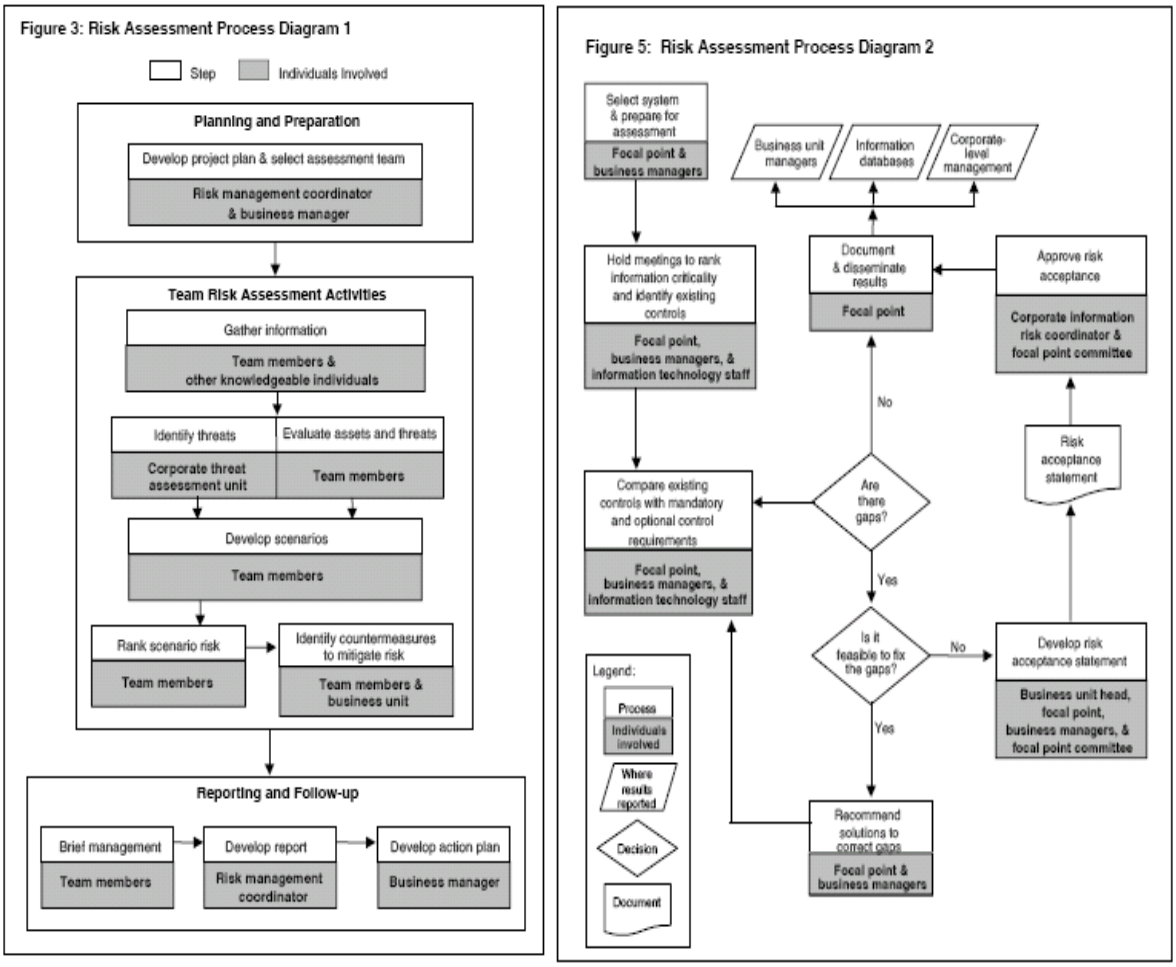


Figure 10: Risk assessment project approaches

Within the *Conducting the Risk Assessment* phase, a standardised approach for risk discovery, analysis and evaluation should be used. Australian Standard 4360: Risk Management Standard is recognised globally as a best-practice methodology for assessment of risks. According to the standard, risk is measured as a product of likelihood and consequence of the particular risk event. The risk-analysis component within AS 4360 has three steps.

- identify risk
- analyse risk
- evaluate risk.

Identify risk

The objective of risk identification is to cover the breadth of possible issues which may impact on the business and develop a distinct list of significant scenarios. When identifying risks, a comprehensive identification process using a well-structured systematic process is critical. Where risks are not effectively identified during this stage, they may be excluded from further analysis. The key questions to answer include[10]:

- What can happen, where and when?
- Why and how can it happen?

Checklists, flowcharts and other tools can be used to identify both assets and events that might be impacted as well as the potential causes of events. Assets and trends discussed in the *Establishing context* section should be considered so that the identification process is forward-thinking. A specific method for comprehensive identification may be the use of a threat or issue tree. The mutually exclusive and collectively exhaustive (MECE)[25] analysis technique can be utilised to categorise potential issues and then drill down further. An example of this process is shown as follows:

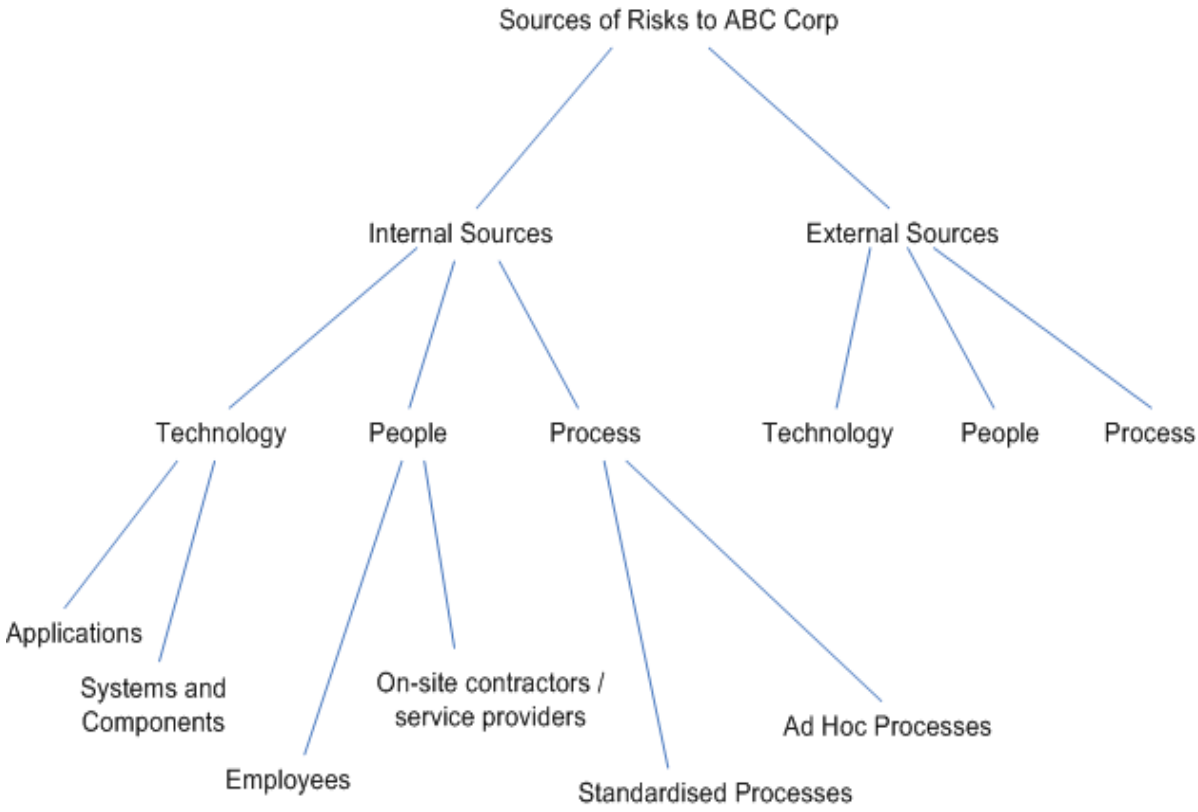


Figure 11: MECE risk-analysis tree

In general, two primary methods of risk discovery can be used—inductive and deductive. Inductive analysis describes a macro-to-micro approach where the threat environment is considered and interpretations of this are then transposed onto the business environment. Deductive analysis occurs in the opposite micro-to-macro direction, where the business requirement or the risk propensity of the business determines the threats that are valid to the specific system or information and thus must be considered.

A combination of the two can be used to draw consensus and triangulate an accurate set of possible risk areas.

[25] AusThink, *MECE – Mutually Exclusive*, November 2006, www.austhink.com/reason/tutorials/Tutorial_6/5_MECE_ME/mece_me.htm

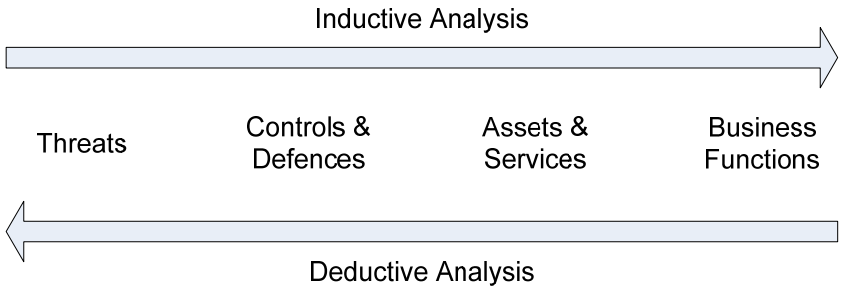


Figure 12: Inductive and deductive threat analysis models

Another way of viewing inductive and deductive threat analysis models is through threat modelling, which can be used as a method of prioritising security investments and securing the most vulnerable components in a system or organisation. Threat modelling can be approached in two general ways:

- attacker-centric
- system-centric.

The attacker-centric model starts with the adversaries and motivations detailed in the *Establish context* section, identifies the likely assets that the adversary would pursue, and from this analyses the likely ways in which this adversary would attempt to gain access to the asset. This is similar to inductive analysis.

The system-centric model reverses this approach, starting with the critical assets as also identified above, and then proceeds to seek out attacks against each component of that asset, independent of the likely adversary. This is similar to deductive analysis.

Once identified, there are several ways to categorise electronic threats. One such method is the STRIDE classification, which considers threats within the following six categories:

- **S**poofing—an illegitimate entity masquerades as a legitimate entity to feign authenticity.
- **T**ampering—a legitimate entity is manipulated by an unauthorised party.
- **R**epudiation—a threat where it is impossible to assert the validity of a transaction.
- **I**nformation disclosure—information is revealed to unauthorised parties.
- **D**enial of service—the availability of a resource becomes highly restricted or unusable.
- **E**levation of privileges—a user gains unauthorised privileges (e.g. ability to perform certain operations or view certain data) beyond their assigned role.

After threat classification, threat rating is performed using the DREAD model[26] which identifies:

- **D**amage potential—a measure of how much damage could occur should the threat take place. The higher the damage, the higher the rating.
- **R**eproducibility—a measure of how easy it is to perform the underlying attack that causes the threat. The easier it is to perform the attack, the higher the rating.

[26] Open Web Application Security Forum (OWASP), *Threat Risk Modelling*, March 2008, www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

- **E**xploitability—a measure of the skill level required to exploit the threat. The less skill required, the higher the rating.
- **A**ffected users—a measure of how many users will be affected. The higher the number of users affected, the higher the rating.
- **D**iscoverability—a measure of how easy it is to discover the threat's existence on a given system. The easier it is to discover, the higher the rating.

The information provided in the previous section *Establishing context* provides a foundation for determining the threat environment and the strategic business requirements for risk management. By considering both inductive and deductive approaches and through completing a threat classification exercise, the consolidated set of risks will provide a greater degree of validity to the business in the context of today's threat environment.

Analyse risk

The objective of this phase is to develop an understanding of the listed risks such that risk treatment strategies can be appropriate and cost-effective. The analysis process involves consideration of the sources of risk, their consequence and the likelihood that those consequences will occur[10]. Preliminary considerations may elect to discard risks that are similar or of low impact. Existing controls should be taken into account when conducting the assessment.

Consequences and likelihood

Within risk management, the 'consequence' of a risk is defined as the outcome or impact of the risk event. 'Likelihood' describes the probability or frequency of that event. These measurements can be derived quantitatively or qualitatively.

When estimating consequence and likelihood, sources of information may include the following:

- past records
- practice and relevant experience
- relevant published literature
- market research
- results of public consultation
- experiments and prototypes
- economic, engineering or other models
- specialist and expert judgments.

Risk analysis can be conducted with varying degrees of detail, and a combination of both qualitative and quantitative information depending on the ease of sourcing the information and its timeliness and usefulness for the overall business purpose. Some tools for deriving the required information include:

- structured interviews with experts in the area of interest
- use of multi-disciplinary groups of experts through inter-departmental workshops
- individual evaluations using questionnaires
- use of models and simulations.

Consequence and likelihood

Consequence is the outcome or impact of an event and is considered in relation to the achievement of objectives. A single event may have multiple consequences, both negative and positive.

Likelihood is used as a general description of probability or frequency. Likelihood is often used as a synonym for probability and frequency especially in a qualitative context.

Adapted from AS 4360

Assessment methods

In general, information security risk assessments contain three components[27]:

- information asset assessment
- threat assessment
- vulnerability assessment.

Understanding assets

Information asset assessment seeks to determine the value of information assets to the business as well as their interdependencies. Only when the value of the assets is determined can the necessary level of protection be formulated. Asset definition provides for the scope of the risk assessment, thus identification of all relevant physical, information and intangible asset types described in *Establish context* is required. The value assigned to an asset should consider the potential cost of obtaining and maintaining the asset as well as the adverse business impact arising from a loss of confidentiality, integrity, availability, accountability, authenticity or reliability[27].

Identification and consideration of asset dependencies is another core component of determining the value of an information asset. For example, the value of an application system is dependent on the value of the data which it holds or processes.

As a general rule, the following can be applied to the value assessment[27]:

- If value of the dependent assets is lower or equivalent to the value of the asset considered, its value remains the same.
- If the value of the dependent assets is greater than the asset considered, the asset value should be increased either as a function of the dependent component or be equal to that of the dependent asset.

[27] Standards Australia, *HB231 Information Security Risk Management Guidelines*, 2004.

Understanding threats

Threat assessment is necessary to determine that no relevant threats are overlooked. The end result of this process is a list of threats identified, their targets and likelihood.

Input to threat assessment should be obtained from:

- asset owners or users
- personnel department staff
- facility planning
- IT specialists
- people responsible for organisational security.

A list of possible threats is generally helpful to perform the threat assessment, although each organisation faces different threats and threats constantly change: the threats faced by organisations today vary significantly from those faced 20 years ago. Possible threats may include:

- errors and omissions
- fraud and theft
- employee sabotage
- loss of physical and infrastructure support
- malicious hacking
- malicious code
- industrial espionage
- additional emerging threats as documented in the *Monitor and review* section of this report.

After identifying any potential threat sources and targets, it is necessary to assess the likelihood of the threats according to:

- threat frequency, based on experience or statistics (see Emerging risks in *Monitor and review*).
- threat motivation (see Threat environment in *Establish context*), necessary capabilities, resources available to attackers, perception of attractiveness and vulnerability of information assets for the possible attacker and for deliberate threat sources.
- geographical factors which may contribute to accidental threat sources—proximity to chemical plants, weather, factors that influence human error or equipment malfunction.

Understanding vulnerabilities

Vulnerability assessment is necessary to determine potential inadequacies within assets which may result in easy circumvention of controls. The results of vulnerability assessment should be a list of vulnerabilities and assessments of their ease of exploitation. Vulnerability assessment involves identifying weaknesses in the:

- physical environment

- organisation—procedures, personnel, management, administration
- infrastructure—hardware, software, communications equipment.

Input for vulnerability assessment should be obtained from:

- asset owners or users
- facility specialists
- IT systems experts on hardware and software.

Examples of vulnerabilities include[27]:

- unprotected connections
- processes for identifying remote users
- untrained users
- wrong selection and use of passwords
- weak access control
- insecure or incomplete backup policy
- location in an area susceptible to flooding.

In assessing vulnerabilities their ease of exploitation is determined. Some assets are easily disposed of, easily concealed, or easily transported—all of these properties can relate to the vulnerability's ease of exploitation.

Each vulnerability should be assessed in relation to each threat that might exploit it in a particular situation: for example, a system may be vulnerable both to masquerading of user identity and misuse of resources. However, the vulnerability to masquerading of user identity may be high because of a lack of user authentication, but the vulnerability to misuse of resources may be low simply because it is difficult to misuse the resources.

Evaluate risk

The evaluation process provides the foundations for treatment methods and priorities. Risk evaluation requires the comparison of identified risks with pre-determined criteria.

The objectives of the organisation and the extent of opportunity should be considered in evaluating risk—where higher potential benefits are associated with higher potential risk, a decision needs to be made taking the organisation's context into account.

The suggested criteria in AS 4360 are presented in **Table 2**.

Likelihood	Consequence: Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	High	High	Very High	Very High
Likely	Medium	Medium	High	High	Very High
Moderate	Low	Medium	High	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium	High

Table 2: AS4360 risk rating levels

Risk rankings provide an indication of the importance to the organisation of risk scenarios identified. The rankings provide an outline for managers to provide recommendations and develop action plans in order of priority. Generally, high-ranking risks are to be dealt with first with another layer of priority given to remediation strategies which are simpler to implement and less resource-intensive. The following section, *Implementing defence in depth*, provides an overview of possible layered security controls that can be considered.

Key success factors

In completing an effective and successful information security risk assessment, a number of factors require close attention. The following have been identified by as critical success factors by the US Government Accountability Office:

- **Obtaining senior management support and involvement**—management buy-in is critical to propagating risk assessment and remediation responsibilities throughout the organisation.
- **Designating focal points**—success is more likely when groups or individuals are designated as focal points to oversee and guide the risk-assessment processes.
- **Defining procedures and tools**—defined and documented procedures are needed for conducting risk assessments in order to standardise assessment processes.
- **Involving business and technical experts**—knowledge and expertise from a wide range of sources are essential to ensure all important risk factors are considered.
- **Holding business units responsible**—in order to propagate a culture of managing information security risk, responsibility for initiating and conducting assessments and implementing recommendations should lie with individual business units.
- **Limiting scope of individual assessments**—once processes and metrics are standardised, organisations should conduct a series of narrow assessments rather than one that attempts to cover all businesses areas.

- **Documenting and maintaining results**—documentation of results allows for managers to be held accountable for the maintenance of certain recommendations. These results can also serve as input for subsequent assessments.

Assessment methodologies and tools

Assessing governance risks

Governance controls are vital for ensuring alignment of the people, process and technology environments in a defence in depth strategy and to facilitate effective decision-making. Because of the nature of governance, poor management of risks in this area can cause a number of negative flow-on effects to the underlying pillars of people, process and technology. Positioned correctly, governance can bridge the divide between IT and business / financial risks.

Assessing governance level risks requires consideration of the underlying objectives of governance. These areas will formulate the key risk domains within which an organisation can focus further on identification, analysis, evaluation and remediation endeavours.

Challenges

Key challenges of assessing governance risk include:

- management buy-in and cooperation
- aligning IT risks with business strategy
- changing industry regulation requirements
- difficulty in defining scope of risks
- difficulty in accurately measuring effectiveness of governance controls
- lack of empirical results
- effectiveness in communication of controls
- requirements for regular internal and external audit.

These challenges can be best managed by ensuring senior executive ownership of information security governance and assessment of performance in managing information security risk at a board or senior executive level.

Approaches

Identifying governance risks requires coordination and participation from the CIO and relevant risk-management advisory boards. Tools which these parties can use to identify existing and potential risks are described below:

- ***Benchmarking***—identification of weaknesses in governance components through comparison against industry standards. Benchmarking can provide valuable input into classification and prioritisation of risks.
- ***Workshops***—with participation of senior executives, workshops enable a business-driven context to be established. Key actions include reviewing strategic positioning, identification of risks in existing governance models and consideration of changes introduced by future governance models.
- ***Documentation review***—review of existing governance policy and procedures. While a less onerous process of review for the organisation, the review does not necessarily validate staff practice where actual controls are not in line with documented requirements.

Vulnerabilities and threats should be identified within the categories of regulatory risk and strategic risk. Examples of vulnerabilities and threats identified in relation to governance are included in the tables below but a more exhaustive list should be collated specific to each organisation.

Sample vulnerabilities and classification	
Lack of monitoring of information security performance	[operational]
Inconsistent security controls across the organisation	[operational]
Exposure through inappropriate security culture	[operational]

Table 3: Sample governance vulnerabilities and classification

Sample threats and classification	
Legal exposure due to non-compliance	[legal]
Financial loss due to fines for regulatory non-compliance	[financial]
Adverse media representation from security incident	[brand/media]
Inappropriate alignment of IT and business strategy	[technical]
Unavailability of CI services due to security incident	[social]

Table 4: Sample governance threats and classification

Detailed analysis

Governance-related risks should be prioritised for future mitigation undertakings. The following describes a methodology for completing this.

Classification of the impact and likelihood of each risk. When performing impact analysis, focus should be placed on risks which involve business mission and strategy, and critical infrastructure services and assets in their coverage. Impacts can be categorised into the following areas:

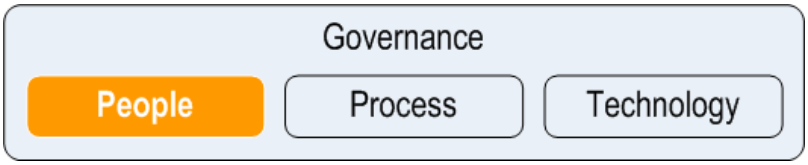
- operational
- technical
- financial
- legal
- brand/media
- social
- other.

Business requirements for residual risk. After mitigating controls are put into practice, there may still be residual risk to critical infrastructure or the business mission, and in such cases the residual risk must be accounted for and either accepted or further addressed. In this phase, a definition is set for the maximum acceptable residual risk which can be absorbed without remedial action, based on the organisation's defined risk-tolerance level.

Assessing cost-effectiveness of mitigating risks. Planning, developing and implementing mitigating controls can develop into a resource-intensive process. Performing a quantitative analysis of the risks involved and comparing this with estimated remediation costs can help support a cost-benefit analysis of projected mitigation costs with risk of loss.

Risk rating. Development of a risk matrix highlighting the severity of a risk based on the likelihood and impact of the risk occurring will allow risks to be consistently prioritised. The output of a risk matrix is an overall rating that can be associated with each risk.

Assessing people risks



Assessing risk exposure arising from *people* requires the organisation to consider both the internal and external environment within which it operates. Risks attributable to people may occur from either accidental exposure (e.g. carelessness) or as a result of mischievous activity (e.g. social engineering). Both types of exposure must be assessed and managed.

Defence in depth controls provided by *governance*, *process*, and *technology* are worth little if inadequate risk management has been adopted for the organisation's people.

The *governance* framework provides direction for establishing a culture of security and these methods must be considered when assessing personnel for vulnerabilities and threats.

The risk assessment of people should be conducted with consideration of how people interact with the organisation, the purpose of their interaction and the type of information systems/assets available to them (i.e. the social environment)[28]. As identified in *Establish context*, 'people' includes employees, contractors, business partners and customers.

Approaches

Various tools may be used to assist the identification of risks associated with the organisation's personnel. These tools utilise screening methods and surveys to identify both existing and potential risks.

- ***Roles assessment***—an analysis of job roles within the organisation, with emphasis on those roles that have greater opportunity of causing harm, e.g. system administrators. The assessment identifies existing risks in the organisation and explores the impact of organisational hierarchy on the risk profile[28]. Such an assessment should also be conducted to evaluate the appropriateness of outsourcing activities to third parties.
- ***Screening tools***—a set of tools that are developed and used by HR during interview of potential employees and may include industry-specific requirements. This may be achieved with customised screening check lists, criminal records checks or questioning referees. Screening tools may also be used for assessing the appropriateness of other personnel interactions before they occur, e.g. assessment of contractors.
- ***Survey/questionnaire—***used periodically to identify changes in the internal environment. These tools may be used to assess the awareness of security processes and thus identify risks attributable to an ineffective culture of security (i.e. assess effectiveness of training/education programs), and assess the effectiveness of the enterprise-wide risk strategy while also facilitating open discussion among personnel.
- ***Incident reports—***identify ongoing risks highlighted by specific incidents, identify causes of exposure and assess how future events may be minimised.
- ***Knowledge risk analysis—***review key personnel who are critical to ongoing business activities, identify if they are the sole holders of core business knowledge, and assess risks associated with personnel departure, knowledge loss or theft (intellectual property or operational knowledge).
- ***Review HR processes—***identify weaknesses in personnel engagement processes and evaluate the effectiveness of exit procedures, and assess training/education provisions and their effectiveness in supporting the security culture.

Vulnerabilities and threats should be identified within the category of insider/outsider, documented and mapped to the resulting outcome. Examples of vulnerabilities and threats identified in relation to personnel are included in the tables below, yet a more exhaustive list should be collated as part of this assessment.

[28] Tchankova, L, *Risk Identification – basic stage in Risk Management*, Environment Management and Health, 2002; 13(3):290-297.

Sample vulnerabilities and classification	
Staff poorly trained in confidentiality measures for system access	[operational]
Lax security culture	[operational]

Table 5: Sample people vulnerabilities and classification

Sample threats and classification	
Personnel sabotage of business operations	[operational]
Social engineering	[operational]
Personnel misuse of privileges	[legal]

Table 6: Sample people threats and classification

Detailed analysis

A detailed analysis of vulnerabilities and threats is needed in order to best determine the likelihood and potential impact of the risk. This can be achieved by exploring the way that people perform their job functions, the types of supervision provided, factors that contribute to the motivation of attackers, and the appropriateness of current controls for information systems/assets.

Analysis of people within the organisation (insiders) should be comprehensive and include assessments of:

- key personnel
- handled information
- level of supervision
- termination strategies
- reward and disciplinary procedures
- training
- technical controls.

The detailed analysis should document the features of each vulnerability/threat including:

- the type of exposure
- description of the associated risk
- identification of the job roles affected
- external parties involved
- identification of the information at risk

- supervision/accountability
- other opportunities for exploitation
- associated motivation factors
- existing controls (e.g. HR policy)
- overall likelihood and impact ratings.

Challenges

Key challenges of assessing people risk include:

- determining the accuracy of information provided by staff
- assessing the culture and practices of the organisation as a whole while making allowance for regional and departmental variation
- difficulty in quantifying results with metrics.

These challenges can be best managed by establishing an ongoing dialogue with staff to allow for an improved security culture to be identified over time, and for personnel-related security risks to be identified promptly and confidently.

Assessing process risks

Business processes provide the implementation of an organisation's strategy by guiding day-to-day activities. They also facilitate ongoing risk-management activities by ensuring routine security reviews are conducted.

Assessment must consider the underlying business objectives of each process and ensure that business owners are engaged to best identify potential weaknesses. Processes should be considered as either core to the business mission (i.e. providing critical infrastructure) or as internal service processes (i.e. providing support to core processes)[29]. Accordingly, risks should be identified in these domains.

Figure 13: Relationship between objectives, strategies and process

[29] Price L and Smith A, *Managing Cultural Assets from a Business Perspective*, accessed 2008: www.clir.org/pubs/reports/pub90/appendix1.html

Approaches

Analysis of processes and their risks can be achieved by the use of the following techniques:

- ***Workflow models*—**document the lifecycle of existing business workflow, used as input to a business process assessment.
- ***Business process assessment (BPA)*—**risks may be identified by reviewing normal business processes and resource allocation and their dependence on information systems/services. A framework should be used to guide the BPA[30], including consideration of process: effectiveness, efficiency, confidentiality, integrity, availability, compliance, reliability[31].
- ***Process validation*—**assess the misalignment of process model/strategy and actual implementation, using the BPA as input[32].
- ***Audit security processes*—**an analysis of processes associated with defence in depth controls. Determine levels of compliance with security policy and risks associated with either poor compliance or inadequate policy. Conducted as a method of maintaining process risks at an acceptable level.

Sample vulnerabilities and threats are provided in the tables below:

Sample vulnerabilities and classification	
Change management processes inadequately documented	[operational]
Processes of hiring/firing employees	[legal]
Inadequate incident response management	[operational]

Table 7: Sample process vulnerabilities and classification

Sample threats and classification	
Legacy business processes being used result in ineffective layered security controls	[operational]

Table 8: Sample process threats and classification

[30] Becker et al., *Guidelines for Business Process Modelling*, Business Process Management, 2000; 1806:241-261.
[31] Information Systems Audit and Control Association (ISACA), *COBIT 4.1, Monitor and Evaluate: Process Description*, www.isaca.org
[32] Castellanos et al, *Challenges in Business Process Analysis and Optimization*, Lecture Notes in Computer Science, 2006; 3811:1-10.

Detailed analysis

The BPA provides a foundation for assessing process risk and should be conducted in conjunction with industry best-practice tools such as COBIT[31] and ITIL[33] (the IT Infrastructure Library).

A detailed analysis should identify what impact a given process risk may have on the organisation. This may be determined by reviewing process documentation with management and analysing how business objectives and strategies may be affected. Such an analysis is required to document:

- triggers for process failure
- process dependencies
- impact on business mission
- cost of the risk.

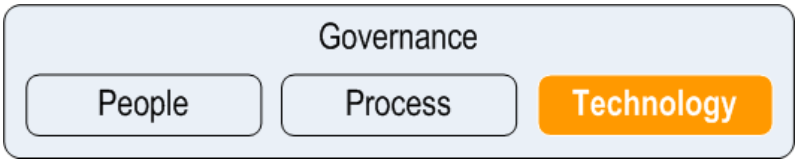
Challenges

Key challenges of assessing process risk include:

- determining the cost of conducting a thorough BPA
- complexity of relationships between procedures, policies, systems and data[34]
- poorly defined/manual processes
- determining documentation requirements
- defining BPA metrics
- difficulty of implementing process changes, based on risk assessment
- appropriateness in selection of services (i.e. changing nature of services available from vendors).

These challenges can be best addressed by prioritising business processes by core objectives, using best-practice frameworks such as COBIT, and ensuring adequate reporting and audit capabilities are provided for monitoring process risk.

Assessing technology risks



Organisations are spending increasing amounts on security, with 98 per cent of respondents to the Deloitte *Global Security Survey 2007* reporting increased security budgets from 2006, and

[33] ITIL, *Information Technology Infrastructure Library (ITIL)*, www.itil-officialsite.com
[34] Minsky S, *The challenge of BPM Adoption*, accessed 2008: www.ebizq.net/topics/bpm/features/5757.html

with 11 per cent of respondents reporting an increase of more than 15 per cent from 2006 security budgets[35].

Assessment of technology risk requires the establishment of formal review processes that will provide assurance of ongoing availability, integrity, and non-repudiation. Technology components should be assessed based on the criticality of business processes they facilitate (i.e. supporting the business mission) and the information which they provide.

An effective assessment of technology risk in a critical infrastructure environment requires a multi-disciplinary approach, calling on the expertise and experience of personnel with backgrounds in IT security, engineering, network architecture and risk management. Business owners must also be included in the assessment of technology risks as their approval must be sought to proceed with implementation of controls and to ensure acceptance of residual risk.

Appropriate policy should be implemented to mandate ongoing technology risk assessment as being part of normal business processes. Inadequate risk assessment may result in significant exposure due to the dynamic nature of enterprise IT services.

Technology risks should be identified by inspecting each layer provided by the defence in depth strategy:

- Technology layers:
  - user
  - application
  - database
  - network
  - operating system
  - physical.

Consideration should also be given to the system's life cycle and the importance of risk assessment at each stage[36]:

- Systems development life cycle (SDLC) stages:
  - design
  - development
  - testing
  - implementation
  - maintenance and review.

Approaches

Assessment of technology risk can be performed using an inductive (start with the threat) or deductive (start with the asset) approach, given that different risks may be identified from each. Vulnerabilities and threats should be identified before documenting actual technology risks.

An organisation's technology environment should be analysed in relation to its impact on business processes as the risk may be accepted by the business for the benefit provided.

---

[35] Deloitte, *Global Security Survey 2007*, www.deloitte.com/dtt/cda/doc/content/ca_en_Global_Security_Survey.final.en.pdf

[36] US NIST, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security), sp 800-2,* 2001, http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf

A combination of tools should be used when assessing technology risk and may include the following:

- ***Load testing and redundancy assessment***—an analysis of the capability of infrastructure to meet business requirements, and an opportunity to identify risks associated with business continuity strategy.
- ***Network penetration testing—***a deductive approach for identifying weaknesses in the perimeter, including firewalls, routers, and IDS.
- ***System penetration testing—***assess system configuration and patching levels to determine potential exposure.
- ***Application review—***analyse critical applications for compliance with secure application development standards (e.g. OWASP[37]). Identify risks relating to authentication, authorisation, input validation, session management, data encryption, error handling and more[38].
- ***Business continuity planning—***review existing processes and identify vulnerabilities in relation to core business objectives.
- ***Technology risk assessment—***utilise a multi-disciplinary team approach to identify risks associated with existing and proposed technology components. Keys to success include the early identification of risks during SDLC to minimise cost, and comparing business benefit with risk exposure[36].

Sample vulnerabilities and classification	
Poor physical security for network infrastructure.	[operational-impact]
Inadequate infrastructure redundancy	[operational-impact]
Default OS configurations in production environment	[technical]
Poorly tested applications implemented	[technical]

Table 9: Sample technology vulnerabilities and classification

Sample threats and classification	
Service failure due to denial-of-service attack	[operational]
Sensitive information leaked	[legal]
Untimely patching processes on production servers	[operational]

Table 10: Sample technology threats and classification

[37] Open Web Application Security Project (OWASP), *OWASP Guide 2.1*, accessed 2008: www.owasp.org
[38] Sivanandhan H, *Application Security Cheat Sheet*, accessed 2008: www.securitydocs.com/library/3387

Detailed analysis

The defence in depth strategy fosters implementation of layered controls and as such, risks must be considered for their weaknesses within this structure. In particular, a detailed analysis should assess ways in which information (or a service) is being used. Analysis should include a review of data:

- transmission
- storage
- protection
- recovery.

An information-centric approach enables technology risk to be mapped to business value, which can be used to document the risk impact. Technology risk likelihood will be affected by existing controls and their effectiveness.

Challenges

Technology is constantly being updated and the threat environment is constantly changing. This makes risk assessment a resource-intensive exercise. Key challenges associated with assessing technology risk include:

- obtaining resources required for testing
- accurately assessing the risk of legacy systems
- accessing business information in unstructured locations (e.g. emails, intranet pages)[39]
- complexity of architecture
- dependency on external networks
- range of third-party devices
- maintenance procedures and reporting
- changing nature of the external threat environment.

These challenges can be best managed by having adequate buy-in from business owners, engaging personnel with a wide range of skills and leveraging the experience of systems architects. Ongoing risk assessment can be achieved through implementation of technology-specific risk reviews, monitoring of trends, media reports and security forums. A prime example of such activity is the Australian Government's Computer Network Vulnerability Assessment Program. The program aims to embody the discussed aspects of risk assessment via ensuring that there are adequate levels of protective security on critical infrastructure systems and networks, minimum single points of failure and tested recovery arrangements.

[39] Warren P and Davies N, *Managing the risks from information- through semantic information management*, BT Technology Journal, 2007; 25(1):178-191.

IMPLEMENTING DEFENCE IN DEPTH

The information security principles from the *Secure Your Information: Secure Your Business* paper relevant to this section are:

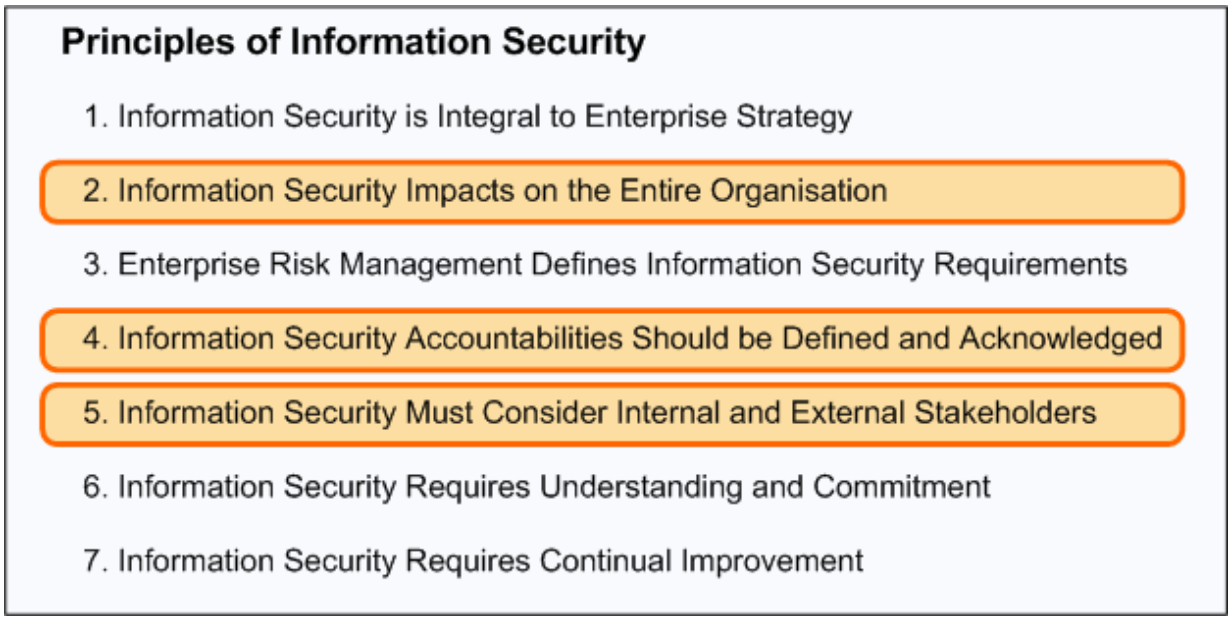


Figure 14: Applicable principles of information security for implementing defence in depth

In order to successfully implement defence in depth in an organisation, management must include the concept within the organisation's strategy, planning and structure. Defence in depth is often considered a principle that underpins *why* certain IT security actions are taken. For further analysis and discussion of the principles of information security, it is recommended that the reader refer to the *Secure Your Information* papers prepared for the IT Security Expert Advisory Group (ITSEAG), available from www.tisn.gov.au.

This paper deals with the implementation of defence in depth at a strategic, principle-based level and provides additional guidance on specific sets of controls that may be applicable to support an organisation's defence in depth initiatives. The section is presented as follows:

- **Core principles—**details the key principles underlying a successful implementation of a defence in depth strategy.
- **Implementing governance controls**—details the key objectives and approaches to integrating defence in depth concepts within the area of information security governance and the key controls available to an organisation in this area.
- **Implementing people controls**—details the key objectives and approaches to integrating defence in depth concepts within the area of personnel security and the key controls available to an organisation in this area.
- **Implementing process controls**—details the key objectives and approaches to integrating defence in depth concepts through operations and procedures in the organisation and the key controls available to an organisation in this area.

- **Implementing technology controls**—details the key objectives and approaches to integrating defence in depth concepts into technical architecture, design and implementation and the key controls available to an organisation in this area.

Core principles

The four core principles of a defence in depth strategy are:

- Implement measures according to business risks.
- A layered approach should be implemented such that the failure of a single control will not result in a full system compromise.
- Controls should serve to increase the cost of an attack.
- Implement technical, procedural and operational controls.

Implement measures according to business risks

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 implementation of a defence in depth strategy requires the organisation to have an understanding of business goals, potential threats and vulnerabilities and the relative risk of each. This allows the defence in depth controls used to treat the risk to be proportional to the business impact of the risk.

An additional concept related to the use of business risk in determining appropriate defence in depth controls, is the need to defend those who cannot defend themselves[40]—for example, business units with inferior technology or security infrastructure. As the defence in depth concept requires an organisation-wide view of risk, the consideration of such items ensures that risks are not being narrowly interpreted and accepted while introducing unacceptable risk to the organisation as a whole.

The elements of evaluating the risk context and risk analysis are dealt with further in previous sections of this report.

Implement controls using a layered approach

Arguably the best-known and most significant of the defence in depth principles is the concept of implementing a layered approach to controls. These layers should have a number of specific attributes:

- **The failure of any single control will not result in a full system compromise**—all IT systems and operational processes can be subject to errors, omissions, flaws in design and implementation or malicious tampering. As a result, it is necessary to ensure that layers of control are implemented such that the failure or subversion of any single control will not

[40] US NSA, *Information Systems Security Engineering*, accessed 2008, www.nsa.gov/ia/government/isse.cfm?MenuID=10.3.2

result in a full system compromise. In order to achieve this, the controls should be mutually supporting and layered in depth[41].

- **Controls should guard against the unknown weaknesses of a layer**—in order for the layered approach described above to be effective, it is necessary for each layer to provide new and different challenges to an attacker and to provide protection against threats that have not yet been addressed by other controls[42].
- **Layers of control are to be considered holistically**—while each layer is providing a new and independent set of controls, it is also important that the full suite of layers and controls is considered holistically to ensure that the ultimate aim of risk minimisation is to be achieved.

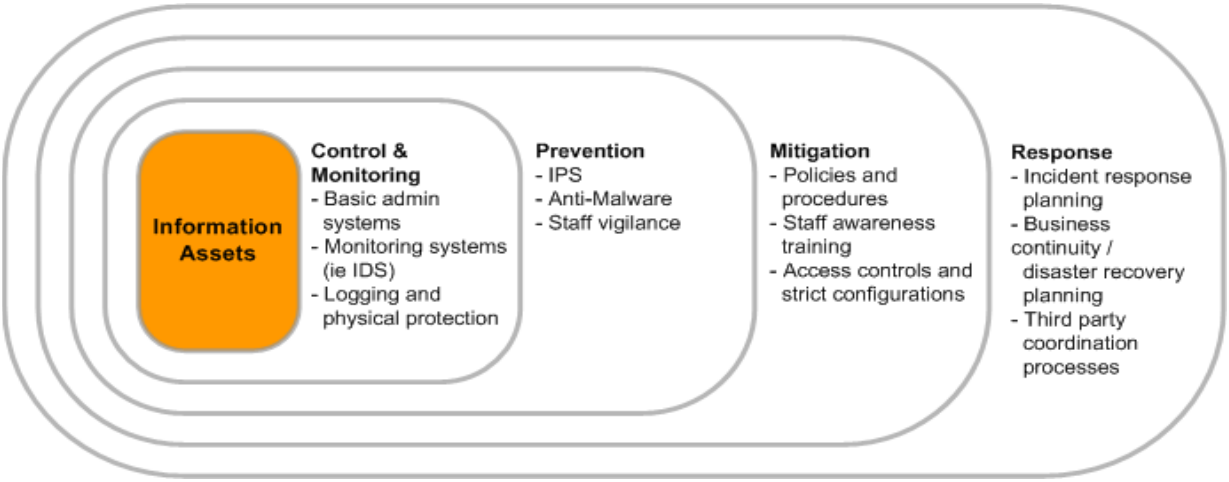


Figure 15: Layer of protection analysis (LOPA)—control layers

Design considerations for additional layers include ensuring that each layer is[43]:

- autonomous
- adequate
- complete
- dynamic
- well-coordinated
- verified.

Controls should serve to increase the cost of an attack

An attacker with infinite time and resources will eventually find a way to compromise any given system or organisation. Fortunately, such infinite time and resources do not exist,

[41] Robinson D. *Defense in Depth: A Small University Takes Up the Challenge*, SANS, Case Studies, 2002, www.sans.org/reading_room/whitepapers/casestudies/710.php
[42] Brooke P, *Building an In-Depth Defense*, Network Computing, 2001,www.networkcomputing.com/1214/1214ws1.html
[43] Republique Francaise Premier Ministre, *In Depth Defence applied to Information Systems: Memo* www.ssi.gouv.fr/en/confidence/documents/methods/mementodep-V1.1_en.pdf

meaning that for the vast majority of attackers there is a cost-benefit determination to be made with regard to starting or continuing an attack against a system or organisation.

In order to lower the likelihood of such an attack occurring, either the benefit of success for the attacker can be reduced or the cost of completing the attack can be increased. A valuable way in which to view information security controls is thus as increasing the cost of an attack, either through requiring additional effort, time, investment, or tools on the part of the attacker. The ultimate aim of such an approach is to make the cost of an attack unacceptable to a potential attacker.

Implement technical, procedural and operational controls

People are a crucial part of any information system and, as a result, are a crucial part of any information security control structure. In order for defence in depth to be effectively implemented it is necessary for controls to be implemented that provide both technical protection as well as procedural and operational management control.

This report is predominantly based on this requirement and structured to consistently deal with the four pillars of control:

- governance
- people
- process
- technology.

Implementing governance controls

Information security governance is the process of establishing and maintaining a framework, and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives[44].

TISN released a paper in July 2006, entitled *Leading Practices and Guidelines for Enterprise Security Governance*[45] 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.

Within a defence in depth model, governance ensures the necessary value is obtained from the overall implementation to ensure success. This can include:

- improved efficiencies
- ensuring consistency with the business mission
- compliance management

---

[44] US NIST, *Information Security Handbook: A Guide for Managers sp800-100*, 2006, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[45] *Leading Practices and Guidelines for Enterprise Security Governance* , 2006, www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~IT+Security+&+Governance.pdf/$file/IT+Security+&+Governance.pdf

- providing a dynamic framework to address challenges associated with ongoing change in the internal and external environments.

The key elements for providing effective governance of a defence in depth approach to information security are:

- accountability—clearly define roles and responsibilities and identify stakeholders.
- risk management—as detailed in the *Establish context* and *Risk analysis* sections of this report.
- policy and compliance management—including legal and regulatory compliance requirements.

There is a need to ensure consistency between elements of the governance model and the risk analysis phase conducted previously. Consistency should exist between IT security policies and risk areas identified from the *Establish context* and *Risk analysis* phases of the organisation's defence in depth initiative.

Accountability

One of the most critical items at a governance level for implementing defence in depth is the commitment of and visible support from senior management. Senior and executive management have a number of specific roles in the governance of a defence in depth program, including providing business input to the:

- risk identification and risk analysis components described in the *Risk analysis* section of this report
- cost models
- modelling behaviours.

This is reflected by Information Security Principle 4 within the *Secure Your Information* papers from the TISN. This principle states that 'information security accountabilities must be defined and acknowledged'. Specific recommendations within this principle include[12]:

- holding executive management accountable for the state of enterprise information security
- assigning information security responsibilities throughout the organisation
- allocating responsibility for information security to match business roles
- defining information security responsibilities for external parties in the engagement contract.

Policy and compliance management

As detailed within the *Establish context* section of this report, any defence in depth strategy will exist within the broader objectives and goals of the organisation and the external environment applicable to that organisation, including legal and regulatory considerations.

While policy and compliance management is primarily a governance consideration, it is of significant importance as it also sets the expectation around risk management and information security management within the organisation. It is a key element in supporting the development and maintenance of a culture of security.

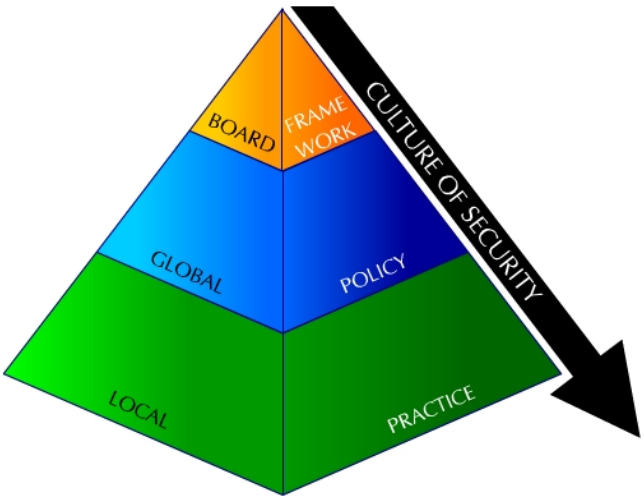


Figure 16: Top-down definition of framework, policy and procedures

IT security standards provide an important measure for determining if a ‘problem’ has occurred. Standards should be re-evaluated periodically to prevent unnecessary ‘false positives’ as equipment changes and expected system and personnel behaviours change through time.

Control analysis

Specific controls in the area of information security governance for defence in depth include:

- risk management
- policy and compliance management
- information security.

The following tables discuss these points in detail.

Focus area guideline: Risk management	
Description	Risk management comprises the business processes and policy framework for identifying threats to an organisation, determining their business risk and implementing mitigation strategies to reduce levels of risk to acceptable levels.
Objectives	• Identify vulnerabilities and threats • Determine business risks and protect the organisation from those risks • Facilitate business acceptance of residual risk • Provide input to business continuity planning (BCP) • Support business units in ongoing risk-management activities

Key controls	• Risk management framework and policy
	• Risk assessment process
	  o identify and classify risks
	  o implement risk mitigation strategies
	  o attain business acceptance of residual risk
	• Risk management standards
	• Documentation of residual risks and risk decisions
	• Awareness of risk management methods

Layered controls	• Risk policy enforcement • Mitigation of risks by addressing both likelihood and impact • Education of management and personnel • Business continuity planning

Implementation	• Develop internal policy for risk management
	  o Engage stakeholders
	  o Define risk priorities
	  o Determine scope of risk analysis
	  o Enterprise-wide framework
	• Evaluate the risk environment
	  o Conduct a risk workshop with stakeholders and risk experts
	  o Asset valuation and prioritisation
	• Assess the internal and external environments
	  o Threats
	  o Vulnerabilities
	  o Exposures
	• Determine business risks
	  o Classify risks
	  ▪ Governance, people, processes
	  ▪ Technology (e.g. infrastructure, network, system)
	  o Assess likelihood of risk incidence
	  o Assess impact of the risk on business function
	  o Allocate a ‘risk score’
	  ▪ Standardised risk matrix (i.e. *risk* = *impact* x *likelihood*)
	• Prioritise and mitigate risks
	  o Map risks to key business objectives/mission
	  ▪ Focus on high-risk items

	▪ Current controls ▪ Recommended controls o Determine residual risk ▪ Review cost-effectiveness of mitigating controls ▪ Attain business acceptance of residual risk o Identify redundancy requirements ▪ Provide input to BCP strategy • Implement controls • Review effectiveness of controls • Provide risk reporting for management • Assist business units for ongoing risk management o Integrate with SDLC o Develop a risk review process o Conduct training seminars o Develop risk management guidelines for business units
Maintenance	• Review effectiveness of mitigation strategies • Assess changes in the risk environment • Address changes in business objectives/desired risk profile
Further Information	• Standards Australia: Australian Standard 4360 Risk Management Portal, accessed 2008: http://www.riskmanagement.com.au/ • Stoneburner et al., 'Risk Management Guide for Information Technology Systems', NIST Publication 800-30, 2002: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Focus area guideline 1: Risk management

Focus area guideline: Policy and compliance management	
Description	Policy and compliance management is the development and ongoing maintenance of policy to support an organisation's mission and to meet identified regulatory obligations.
Objectives	• Identify and meet regulatory obligations • Ensure stakeholders are responsible and accountable • Instil secure behavioural change and competence • Monitor and report security performance

Key controls	• Policy development
	  o Australian Standards for AS3806 Compliance Programs
	  o COBIT
	• Policy alignment with risk management strategy
	• Enforcement through compliance monitoring
	• Policy review
	  o Alignment with business strategy
	  o Meet regulatory requirements

Layered controls	• Policy compliance enforced through both internal and external audit reviews

Implementation	• Initiate project
	  o Define authorship
	  o Accountability and responsibility
	  o Risk-based focus
	  o Identify operational efficiencies
	• Engage stakeholders
	  o Accountability and responsibility
	  o Identify core business objectives
	  o Facilitate a culture of security
	  o Resource commitment for development and implementation
	• Assess existing governance framework
	  o Identify policy strengths and weaknesses
	  o Assess compliance
	  o Review reporting requirements
	• Policy development
	  o Scope/application definition
	  ▪ Enterprise-wide
	  ▪ Clearly defined policy objectives
	  ▪ Assignment of responsibilities
	  ▪ Identify regulatory obligations
	  o Framework
	  ▪ Use best-practice governance tools (e.g. COBIT)
	  ▪ Support business objectives
	  ▪ Measurable outcomes
	  o Documentation
	  ▪ Policy ownership

	▪ Audience, accountabilities, objectives, purpose, description ▪ References to other related policies • Policy implementation o Communicate key requirements and deadlines o Provide resources to facilitate compliance o Training • Assess compliance o Develop audit processes o Compliance reporting o Recommendations to achieve compliance
Maintenance	• Review policy to support business direction • Assess policy compliance o Enforce policy through administration of penalties o Support compliance through training, education and provision of resources • Review effectiveness of policy and alignment with business strategy
Further Information	• Australian Compliance Institute, 'A3806 Practitioner Resources', accessed 2008: http://www.compliance.org.au/www_aci/default.asp?menuid=124 • Allen, J, Westby, J, 'Characteristics of Effective Security Governance', CERT publication, 2007, www.cert.org/archive/pdf/GES_IG_1_0702.pdf • Allen, J, Westby, J, 'Defining an Effective Enterprise Security Program', CERT publication, 2007, www.cert.org/archive/pdf/GES_IG_2_0703.pdf • Bowen et al., 'Information Security Handbook: A Guide for Managers', NIST publication 800-100, 2006: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

Focus area guideline 2: Policy and compliance management

Focus area guideline: Information security	
Description	Information security is the set of business processes and controls that provides assurance of confidentiality, integrity and availability of information within an organisation.

Objectives	• Provide assurance of system security properties
	  o Confidentiality
	  o Integrity
	  o Availability
	• Assess, understand and accept residual risk
	  o Engage business owners
	  o Facilitate decision-making
	• Promote information security awareness

Key controls	• Information security management framework based on information security principles
	• Systems classification process covering:
	  o Business function
	  o System dependencies
	  o Information sensitivity
	• Security requirements
	  o Baseline (i.e. based on system classification)
	  o Tailored (i.e. recommendations based on security principles)
	  o Systems evaluation
	• Security documentation and training

Layered controls	• Information-centric review process
	• Authorisation review process
	  o Input from multiple personnel
	  o Security, architecture, engineering and business input

Implementation	• Assess information use
	  o Business functionality
	  o Information classification
	  ▪ Intellectual property
	  ▪ Business objectives/mission
	  ▪ Sensitive information
	  o Review compliance requirements
	  ▪ Privacy legislation
	  ▪ Industrial regulations
	• Develop information security requirements
	  o Allocate appropriate resources
	  ▪ Security personnel
	  ▪ Architecture personnel
	  o Discuss risk profile with management
	  ▪ Define baseline/mandatory controls
	  o Identify mandatory controls based on DiD principles
	  ▪ Existing network/systems

	▪ Proposed system or network enhancements • Establish information systems review process o Supporting documentation ▪ Policy references ▪ Process requirements • Conduct information security review o Assess impact on business mission ▪ Prioritisation ▪ Potential exposure o Internal/external system dependencies o Compliance with information security requirements o Authorisation to operate (ATO) process ▪ Categorise information system ▪ Forum for discussion of security risks and business benefit ▪ Identify remediation requirements • Conduct in-house training for business units o Support SDLC
Maintenance	• Conduct information system assessments o Implementation exposures o Efficacy of security controls o Compliance with security requirements • Recommend tailored controls • Review and modify ATO process • Update information security documentation
Further information	• Chew et al., 'Information System Security Reference Data Model', NIST publication 800-110 (Draft), 2007: http://csrc.nist.gov/publications/drafts/sp800-110/Draft-SP800-110.pdf • Straub, K, 'Information Security Managing Risk With defence in depth', • SANS Reading Room, accessed 2008: www.sans.org/reading_room/whitepapers/infosec/1224.php • Swanson, M, Guttman, B, 'Generally Accepted Principles and Practices for Securing Information Technology Systems', NIST publication 800-14, 1996, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

Focus area guideline 3: Information security

Implementing people controls

Information security practitioners are faced with the adages 'People are the weakest link'[46] and 'Security is only as good as its weakest link'. Despite this, they may also be the greatest strength when organisations are able to develop an internal culture of security. People have a key role to play in implementing defence in depth, with specific roles including:

- **Executive ownership.** In order for the defence in depth initiative to receive grassroots support and attention, it is crucial for the program to have clear and visible support from senior/executive management.
- **Stakeholders' interests.** In addition to specific executive ownership and support of the defence in depth program, specific stakeholders must have a role in designing, implementing and monitoring controls.
- **Addressing personnel-related risks.** During the risk-analysis phase, personnel-related risks may be identified and controls recommended, such as the vetting of key staff, the introduction of a separation of duties policy, or the introduction of job rotation. All such controls require the commitment and support of staff to be effective.

While periodic audits and assessments may provide validation of network and physical protection, it is difficult to ascertain the robustness of the people element at any discrete point in time. Only a partial view is often possible through assessments such as surveys and social engineering assessments. Furthermore, the variability of human behaviour means defences need to be resilient to fluctuating environmental conditions (e.g. staff morale)[47].

A layered controls approach can be implemented for mitigating people-related risks in the organisation through an employee lifecycle approach, covering the following areas:

- job and role definition
- recruitment and selection
- induction, training and development
- ongoing operations
- role change management
- management of morale
- termination of employment.

Job and role definition

As best practice, security responsibilities are to be clearly placed into job and role descriptions throughout the organisation as a way of formally assigning accountabilities. At an executive level, ownership of the state of security will ensure support for information security initiatives.

A key element in job and role definition is ensuring appropriate separation of duties is maintained. This incorporates the following elements:

[46] Mark R, *Humans Still Weakest Security Link*, 9 Jun 2004, Internet News, http://www.internetnews.com/security/article.php/3366211
[47] Bolman and Deal, *Reframing Organizations*, 2003, Jossey-Bass.

- Dual ownership or authorisation—ensuring that more than one person is required to complete a given task or process, in order to help prevent mistakes, give staff a clear distinction of their duties and ensure that a single staff member acting alone cannot compromise security.
- Sponsor/owner delineation—creating a sponsor's role to provide an audit and review function, while the owner implements the decision upon approval.

Staff usage of information systems can be identified in a single acceptable usage policy (AUP) which applies to all staff. Agreement to the AUP should be a key element of the employment contract. In some instances, the AUP is integrated and becomes an element of the human resources policy framework[48,49]. Key elements of an AUP include:

- correct usage requirements
- a brief understanding of why information security is important and the role of employees
- standard procedures for the reporting and escalation of incidents.

However, the ultimate objective of an AUP is to promote ethical behaviour and employee vigilance[50].

Recruitment and selection

A key selection criterion for many organisations today is 'cultural fit'. In order to develop a culture of security, it is important for this cultural fit to include consideration of risk and security awareness.

The ISO 27002 standard incorporates guidelines for conducting employment screening processes. The standard suggests that while taking into account the relevant privacy and protection of personal data requirements, organisations should include the following, where permissible, for both employment candidates and contractors[51]:

- availability of satisfactory character references
- a check for completeness and accuracy of applicants' *curriculum vitae*
- confirmation of claimed academic and profession qualifications
- independent identity checks
- other more detailed checks, such as credit and criminal checks, where relevant.

Before conducting such processes, details of the recruitment policy should be provided to the potential candidate. The Australian Standard on Employment Screening and associated

[48] Birkbeck University of London, *Human Resources – Network Security Policy*, 2006, www.bbk.ac.uk/hr/policies_services/policies_az/networksecurity
[49] Nolan J, *Best Practices for Establishing an Effective Workplace Policy for Acceptable Computer Usage*, 2005, Information Systems Control Journal.
[50] Robb D, *Protecting Sensitive Data Requires Vigilance: HR and IT Should Work Together To Safeguard Systems From Internal and External Threats*, 2002, HR Magazine, http://search.looksmart.com/p/articles/mi_m3495/is_4_47/ai_84928073
[51] ISO, ISO 27002: 2005, *Information technology - Security techniques - Code of practice for information security management*, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

handbook (AS 4811 and HB 323) can be used as guidance in this area. This standard provides guidance on[52]:

- when security checks should take place
- methods to verify identity, checking CVs, education credentials and police records
- privacy issues, such as who the information can be released to
- training and probity checks on staff employed to do screening.

Induction, training and development

All new employees should be adequately equipped with the knowledge to deal with threats such as phone fraud, email spam and leaving documents on desks when unattended, as well as understand the correct processes for web browsing, emailing at work and conducting anti-virus updates. If roles require additional specific security knowledge, specialised training must be provided to give new users with the knowledge to satisfy their job requirements. This will often be particularly relevant to project managers, business analysts, and technical staff.

Despite the role of human behaviour in influencing information security, only 29 per cent of organisations that participated in a 2007 CompTIA survey suggested that security training was a requirement at their company, and only 32 per cent offered end-user security awareness training of some description[53].

Given the knowledge gap that is widely acknowledged to exist in employee understanding of information security, awareness and training programs are critical for the safeguarding of data[54], and the need to develop a culture of security[55]. Arming staff members with security knowledge to enable them make informed decisions is key to developing this culture.

Training and development is a cyclical process which includes:

- assessment of the knowledge gap
- training program design and planning
- development of training programs
- implementing training programs
- evaluation of training outcomes and reassessment of the knowledge gap.

Successful awareness programs are generally implemented as a continuous initiative, utilising workplace signs, pamphlets and email newsletters as reminders.

The objective of an awareness and training program is not simply to distribute information on procedures to follow and actions to avoid. Training should also be a mechanism to provide an understanding of information security concerns, providing users with the knowledge they need

---

[52] Standards Australia, *New Security Standards Help Protect Community*, www.standards.org.au/downloads/060719_New_security_standards_launched.pdf
[53] CompTIA, *Summary of Information Security: A CompTIA Analysis of IT Security and the Workforce*, CompTIA Research, 2007, www.comptia.org/sections/research/reports/200704-ITSecurity.aspx
[54] Coe K, *Closing the Security Gap*, August 2003, HR Magazine, www.shrm.org/hrmagazine/articles/0803/0803coe.asp
[55] Mendham T, *A Secure Culture*, February/March 2006, CIO Enterprise Focus: Security.

to make correct decisions when new scenarios arise and participate in appropriate risk management processes.

Ongoing operations

The management of information security performance should tie into other HR-related processes, such as job design, recruitment and selection, training and development. Key elements to support information security in day-to-day staff operations include:

- Anonymous reporting—providing facilities for anonymous reporting of incidents or concerns to encourage a culture of vigilance and disclosure.
- Monitoring of personnel—providing early detection of potential threats, as well as ensuring that employees adhere to the prescribed security policy.
- Performance management—using multiple methods with a combination of objective metrics and subjective observation. Employee awareness should be periodically tested through overt and covert security assessments, such as utilising social engineering strategies to examine employee response to potential phone fraud.
- Information sharing—allowing personnel to educate each other on new threats and evaluate their actions in dealing with these threats.
- Job rotation—helping reduce boredom, provide for backup in case of accident or resignation. This can also help security initiatives through identifying fraudulent activity.

Role change management

When staff change roles within the organisation, or the nature of their involvement changes (i.e. from an employee to contractor), there is a need to automatically review their authorisation and access capabilities across the organisation.

When transfers of employment lead to breakdowns in ‘Chinese wall’ implementations, additional criteria and/or controls should be placed on staff. Additional personality assessments may be enforced and the new supervisor provided specific notice or additional review and audit requirements. Staff transfers of this kind may be limited or discouraged altogether.

Managing morale

The human resource function, in conjunction with managers, should manage employee morale to aid information security. By providing services such as counselling and grievance resolution, organisations provide a vehicle for the human resource function and the direct managers to address both on-the-job and personal concerns before they begin to affect an employee’s working performance. By addressing these concerns, organisations limit the potential threat of employees becoming disgruntled, thus reducing the risk of them committing malicious actions or being targets for providing information.

Termination of employment

A key process in information security is the correct removal of information access at the point of staff termination. Whether the circumstance is an amicable or hostile dismissal, or a case of redundancy or resignation, the human resources function should be enacted to manage the

termination process. The key for human resources is to humanise the termination process, avoiding any unnecessary level of employee distress[56].

The human resources responsibility also includes conducting termination interviews. At this stage, the human resources and security functions can seek to identify the potential risk of the outgoing employee taking confidential information for future use[57].

An additional control component is the need for succession planning, particularly when the departing staff member has significant roles in information security. Where possible, extended handover periods should be implemented, along with a practical demonstration of the responsible tasks, rather than a desktop run-through. Additionally, formal documentation of processes should be developed to further the understanding of the newly responsible staff member.

Control analysis

Specific controls in the area of information security people for defence in depth includes personnel security. The following tables discuss this point in detail.

[56] Ross E, 'Sack With Care', 25 January 2006, *Business Review Weekly*.
[57] ISO, ISO 27002: 2005, *Information technology - Security techniques - Code of practice for information security management*, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

Focus area guideline: Personnel security	
Description	Personnel security is the set of business processes and controls that protects an organisation from fraudulent or malicious employee behaviour.
Objectives	• Protect against fraud, espionage, politically motivated attacks • Prevent unauthorised access or use of assets/information • Prevent high-risk personnel from joining the organisation • Protect personnel from harm • Identify and respond to ongoing threats from personnel

Key controls	• Personnel security framework
	  o Screening
	  o Trustworthiness
	  o Capabilities
	• Pre-engagement checks
	  o Pre-employment checks
	  o Secure contracting
	• Engagement processes
	  o Non-disclosure agreements
	  o Travel warnings
	  o Emergency drills
	• Screening for insider potential
	  o Personnel education
	• Access controls

Layered controls	• Pre-engagement and engagement screening • Enterprise-wide awareness campaign

Implementation	• Assess information value to insider/outsiders
	  o Align personnel security controls to risk management strategy
	• Review threats and vulnerabilities
	  o Organisational impact
	  o Wider community impact
	  o Potential for exploitation (harm)
	• Identify opportunity to cause harm
	  o Review employee access to assets/systems
	  ▪ Personnel job roles
	  ▪ Levels of supervision (e.g. administrators vs. cleaners)
	  o Identify potential motives
	  ▪ Financial
	  ▪ Sabotage (i.e. by a competitor)
	  ▪ Espionage (i.e. on behalf of a third party)
	  o Document screening requirements
	  o Provide support for HR processes
	• Conduct screening of personnel
	  o Pre-employment checks
	  ▪ Identity
	  ▪ Employment history

	▪ Convictions ▪ Interviews ▪ Questionnaires (e.g. psychological assessment) o Monitoring ▪ Protective monitoring (e.g. supervision) ▪ Access controls ▪ Intrusion detection • Secure contractor engagement o Pre-contract checks ▪ Secure contract agreement (agency-based checks) ▪ Accreditation ▪ Professional recognition o Monitoring ▪ Assign internal responsibility ▪ Supervision ▪ Staged implementation • Implement engagement processes o Confidentiality (e.g. enforce non-disclosure agreements) o Physical safety (e.g. fire drills) • Implement termination processes o Exit procedures • Implement automated controls o Access controls o Intrusion detection • Develop an education campaign o Assist personnel in identifying manipulation (i.e. social engineering) o Document/publish screening requirements (HR)
Maintenance	• Screening of employees for change o HR process to identify inappropriate behaviour, change in work pattern • Investigation processes o Review mischievous activities o Document findings o Provide input to potential legal proceedings • Audit of policy/procedures • Reporting of personnel security
Further information	• MI5 Security Service Report, ‘Personnel Security: Managing the Risk—2nd edition’, accessed 2008: www.cpni.gov.uk/Docs/Managing_the_Risk_2nd_edition.pdf ▪ CERT Publication, ‘Personnel Security Guidelines’, accessed 2008: www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf

Focus area guideline 4: Personnel security

Implementing process controls

The implementation of a defence in depth strategy requires process controls to be established in three key areas:

- **Protecting** against the threats and mitigating the vulnerabilities.
- **Detecting** security incidents in a timely and effective manner.
- **Reacting** to these incidents in a manner that minimises impact on business operations.

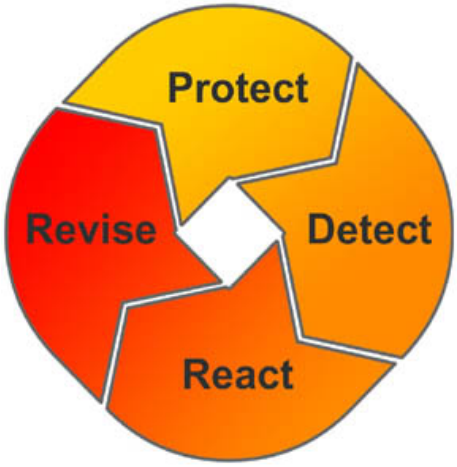


Figure 17: Protect, detect, react, revise model

In addition to these three key areas, there is also an ongoing requirement to **revise** the implemented processes and controls over time. This element is dealt with in more detail in the *Monitor and review* section of this report.

Key to all the following procedural control elements is the need for these to be documented and communicated, and for compliance to be assessed. As such, there is a considerable inter-relationship between the governance elements discussed previously, and the procedural controls set out below.

Protect

Establishing information security procedures to effectively protect information and systems will touch on a wide range of existing functions and teams within the organisation. Controls that can be implemented include:

- **Security maintenance activities—**including tasks such as patch management, vulnerability management, firewall management, Intrusion Detection System (IDS) and system log analysis and related tasks.
- **Integrating security into the systems development lifecycle—**ensuring that all systems are designed with security in mind and developers have security as a key success factor for projects.
- **Change control—**ensuring that all changes to the IT environment are subject to a rigorous risk assessment including information security considerations.

- **Backup and recovery capability development**—extending the simple technical 'backup' requirement to incorporate processes for data recovery, restoration and search.
- **Identity, access and password management**—as the 'gateway' to all information access within an organisation, ensuring robust controls are in place surrounding the allocation of access privileges and the handling of these credentials.
- **Data ownership and security classification**—ensuring that information is 'owned', classified, and consistently secured according to the classification
- **Data retention and disposal**—ensuring that sensitive information no longer required by the organisation is appropriately disposed of, minimising the 'attack surface' presented by unused and unmonitored information.
- **User awareness training**—ensuring that all employees, contractors and other necessary third parties have a consistent understanding of security controls required and implemented and their specific job role as it relates to information security.

Detect

A principle of defence in depth is that in addition to protecting against attacks, it is necessary to expect that such attacks will occur and implement mechanisms to identify them before they succeed. It is also necessary to constantly monitor the organisational environment to detect changes to the security controls in place. Controls that can be implemented to support these detection capabilities include:

- **System testing and audit**—establishing a regular and consistent test regime across all relevant systems within the organisation in order to proactively identify vulnerabilities, assess the associated risk and mitigate as necessary.
- **Anonymous reporting—**also known as 'whistleblowing', can support the identification of issues by employees where they involve personnel in positions of authority.
- **Business continuity plan (BCP)/disaster recovery plan (DRP) testing—**allowing the organisation to assess the degree to which existing BC/DR plans will be effective in allowing recovery in line with business requirements.
- **Security metrics—**the use of security metrics to assess performance over time can identify where either technologies or processes are failing. Such metrics can include the percentage of patches installed in a given month, attacks identified via the IDS, spam email identified as a percentage of all email etc. The actual metrics are best defined by the organisation to reflect the areas of importance.

React

Given the expectation that attacks will occur, robust processes must be established to handle this scenario. Reactions to a security incident can be categorised into four timeframes:

- **Immediate response**—identify that an incident is occurring and identify the source and/or component responsible for the incident.

- **Assessment and activation—**assess the status of the incident, determine the business operations affected, and determine the most appropriate actions.
- **Response/recovery**—execute the necessary actions to stop the incident and recover operations capability.
- **Resumption**—following assessment of the incident's root cause and resolution of necessary issues, resume normal business operation.

Controls that can be implemented to support the organisation's ability to effectively react include:

- **Incident response processes**—ensuring that all necessary stakeholders are aware of the necessary actions in the event of a security incident, including internal and external communication and engagement with groups such as law enforcement, the media and computer emergency response teams (CERTs).
- **Business continuity management—**definition of a business continuity plan or disaster recovery plan, to ensure business operations continue while recovery and resumption activities take place.

Control analysis

Specific controls in the area of information security processes for defence in depth include:

- incident response management
- audit management
- user access management
- identity management.

The following tables discuss these points in detail.

Focus area guideline: Incident response management	
Description	Incident response management is the set of business processes and controls established to minimise the impact of security incidents and limit their recurrence.
Objectives	• Avoid incident occurrence through proactive monitoring and response • Minimise the impact of security incidents • Establish processes to accurately detect policy breaches and provide containment/mitigation • Identify the source of breaches and provide reporting to assist in recourse (forensics, investigation and potential litigation) • Restore system/environment to full operational status and provide assurance of data/system integrity • Provide reporting tools for management

Key controls	• Policies, standards, and procedures
	  o Define incident response service levels
	  o Establish a computer security incident response team (CSIRT)
	  o Assign responsibilities and provide awareness training
	• Identify trusted contacts for communications
	• Intelligence generation (active monitoring of threats)
	  o Logging and log analysis
	  o Trend analysis
	• Incident triage
	  o Interpretation, prioritisation, trend analysis
	• Incident coordination
	  o Categorisation
	  o Cooperation, interaction and disclosure of information (including reporting requirements)
	• Incident resolution
	  o Technical analysis and assistance
	  o Eradication
	  o Recovery

Layered controls	• Information gathering (threat analysis/awareness) • Active monitoring (network device logs) • Incident alarms • Internal staff reporting

Implementation	• Implement controls through a dedicated CSIRT
	  o Appropriate mix of network, host, server, operational security skills
	• Implement a remote intrusion monitoring (RIM) system
	• Develop incident reporting forms (online)
	• Execute security tools
	  o Network (e.g. intrusion detection systems)
	  o Application (e.g. access logs)
	  o Monitoring (e.g. virus scanning)

	• Implement education and training initiatives
	  o Advisories
	  o Presentations and workshops
	  o Security audits
	• Use centralised media communications for incident management

Maintenance	• Post-incident review (PIR) by management
	  o Assess nature of incident (accidental/intentional)
	  o Determine causative factor and identify remediation
	  o Assess effectiveness of response actions
	• Regular audit/review of incident trends
	• Regular testing of incident response technology (e.g. IDS) and process

Further information	• CERT, 'Creating a Computer Security Incident Response Team: A Process for Getting Started', 2006: www.cert.org/csirts/Creating-A-CSIRT.html • Radvanovsky, B, 'Incidence Response Management (An overview of how to respond to security threats)', 2004: www.unixworks.net/papers/wp-013.pdf • Smith, D (AusCERT), 'Forming an Incident Response Team', 1995: www.auscert.org.au/render.html?it=2252 • Brownlee & Guttman, 'Expectations for Computer Security Incident Response', 1998: www.ietf.org/rfc/rfc2350.txt • International Organization for Standardization, 'ISO 27002:2005 Information technology - Security techniques - Code of practice for information security management', Section 13: Information Security Incident Management, 2005.

Focus area guideline 5: Incident response management

Focus area guideline: Audit management	
Description	Audit management is the set of business processes and controls governing departmental and personnel accountability, the evaluation of the appropriateness of implemented controls and the reporting of audit outcomes to management.
Objectives	• Ensure accountability of departments and personnel • Identify duration and metrics for reporting • Evaluate the adequacy and appropriateness of controls • Determine the alignment of security activities and defence in depth strategy • Make management aware of audit outcomes

Key controls	• Defined audit objectives
	• Accountability of audit activities
	• Audit standards/processes/tools
	  o ITIL, CoBIT
	  o Computer-assisted audit tools (CAAT)
	• Continuous audit
	  o Develop understanding of control area
	  o Evaluation of each control
	  o Assess compliance
	  o Substantiate the risk of controls not being met
	• Incidental audit
	  o Analysis of security breaches
	  o Recommendations for remediation

Layered controls	• Third-party review of audit team activities • Audit of people, process, technology (applications and infrastructure) • Internal audit review of testing

Implementation	• Identify audit drivers
	• Define audit scope
	  o Risk analysis (information-centric)
	• Identify suitable audit evidence
	  o Observed processes and physical items
	  o Documentation
	  o Representations
	  o Analysis
	• Gather audit evidence (i.e. enquiry, observation, inspection, confirm, monitor)
	  o Logs (e.g. firewall, IDS, server)
	  o User-access reports for assets/services
	  o Maintenance processes (e.g. virus signatures)
	  o Personnel questionnaire
	  o Site survey
	• Review asset/service breaches

	○ Identify cause and appropriate remediation • Test controls ○ Social controls (e.g. social engineering) ○ Application controls (e.g. authentication controls, malicious code) ○ System controls (e.g. anti-virus maintenance) ○ Network controls (e.g. penetration testing) ○ Physical controls (e.g. access to infrastructure) • Document audit findings, conclusions and recommendations ○ Alert management of potential weaknesses beyond the scope of audit
Maintenance	• Develop an implementation plan for actioning audit items • Develop periodic audit schedule • Debriefing with management for audit process ○ Assess effectiveness of audit process ○ Update audit controls
Further information	• NSA, 'Information Assurance Technical Framework (IATF)', Release 3.0, 2000: www.nsa.gov/snac/support/defenseindepth.pdf • ISACA, 'IS Auditing Procedure: Intrusion Detection System Review Procedure', 2003: www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=31603 • ISACA, 'IS Auditing Guidelines', accessed 2008: www.isaca.org/Template.cfm ?Section=Standards&CONTENTID=40494& TEMPLATE=/ContentManagement/ContentDisplay.cfm • International Organization for Standardization, 'AS/NZS ISO IEC 27001-2006 Information technology - Security techniques - Information security management systems - Requirements', Section 6: Internal ISMS audits, 2006. • International Organization for Standardization, 'ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing', Section 5: Managing an audit programme, 2002.

Focus area guideline 6: Audit management

Focus area guideline: User access management	
Description	User access management is the set of business processes and controls that restricts access to an organisation is information and resources and limits the ability of users to defraud business processes.
Objectives	• Ensure that only authorised users have access to information and resources • Limit damage that can be done by users • Restrict access to what is required for business role • Allow user access to be tracked and audited • Limit the ability for users to defraud processes
Key controls	• Role-based access controls (RBAC) • Access-control lists (ACLs) • Separation of duties • Least privilege • User provisioning process • Authentication using multiple factors • Employee termination process • Logging and auditing
Layered controls	• Requiring authentication (logins) • Physical access (premises security) • Network access (firewalls) • File system access (permissions) • Application access (credentials, OS, firewall) • Application function access (within each app) • Data access (database table/view privileges, within each app, within document repository)

Implementation	• Implement user management infrastructure
	  o Centralised identity store
	  o Directory services
	  o Authentication services
	  o Public key infrastructure
	  o Service desk tracking system to capture access requests and changes
	• Adopt well-defined user management business processes
	  o User provisioning
	  o User termination
	  o Role changes
	  o Password management
	• Design access controls into systems corresponding to threat/risk assessments and information classifications
	• Develop auditing systems and procedures covering
	  o All user access changes
	  o Use of special privileges

	o Authentication attempts and failures
Maintenance	• Implement user account change management process guidelines • Regularly identify and suspend inactive accounts • Conduct regular access reviews to reconcile expected access against actual access levels • Conduct regular review and alerting for access logs • Implement incident response procedures to handle, detect and remediate access breaches
Further information	• Defence Signals Directorate, 'ACSI33 - Australian Government Information and Communications Technology Security Manual', September 2007, www.dsd.gov.au/_lib/pdf_doc/acsi33/acsi33_u_0907.pdf • International Organization for Standardization, 'ISO 27002:2005 Information technology - Security techniques - Code of practice for information security management', Section 11.2: User Access Management, 2005. • Hurst, Jim, 'Are you authorized? Key Theories of Access Control', GIAC Resources, July 2007: www.giac.org/resources/whitepaper/access/422.pdf • TISN, User-Access Management - A Defence in depth control analysis TISN-IN-CONFIDENCE Report, April 2008.

Focus area guideline 7: User access management

Focus area guideline: Identity management	
Description	Identity management is the set of business processes governing the establishment and maintenance of identities for the systems and users that interacts with organisation information and resources.
Objectives	• Accurately identify and authenticate systems and users • Appropriately provision accounts and services • Provide accountability of data access • Protect against and detect fraud

Key controls	• Account/service provisioning policy
	  o Identity assurance levels (i.e. risk-based access requirements)
	  o Trusted administration
	• Identification and authorisation services
	  o Enterprise-wide identity management
	  ▪ Single sign-on (SSO)
	  o Role-based access control
	  o Directory services
	  ▪ LDAP
	  ▪ Digital certificate stores
	  ▪ Key servers
	  o Network access control
	  ▪ IEEE 802.1x
	  ▪ Authentication servers (e.g. RADIUS)
	• Integration standards
	  o Facilitate enterprise-wide identity management (ISO 18876)
	• Identity maintenance
	  o Maintain data integrity
	• Personnel education
	• Fraud protection unit
	  o Monitoring information system access
	  o Identifying mischievous activity
	• Audit reporting

Layered controls	• Additional access controls for high-value information • Encryption of identity information • Enterprise-wide security awareness campaign

Implementation	• Develop identity policies
	  o Least privilege access
	  o Constraints on sensitive information
	  o Provisioning requirements
	  ▪ Define roles and responsibilities
	• Document identity requirements
	  o User authentication
	  ▪ ID/password
	  ▪ Tokens

	▪ Biometrics (e.g. voice, fingerprint, retina) o System authentication o Revocation policy ▪ Account expiry, inactivity, password failures • Account/service provisioning o Develop workflow o Revocation processes o Maintenance processes ▪ Automated alerting/reporting of anomalies • Design and implement identity management services o Select an appropriate technology o Allocation of resources • Educate personnel o Prevent identity theft/misuse o Promote security awareness ▪ Username/password use/disclosure ▪ Document shredding/disposal ▪ Physical access ▪ Privacy legislation ▪ Other threats (e.g. social engineering) • Documentation and training
Maintenance	• Helpdesk support • Fraud prevention o Proactive monitoring of access o Automated anomaly alerts • Change management processes o Maintain data integrity (e.g. minimise duplicate accounts) • Identity audit process
Further information	• COBIT, DS5.3, Identity Management • The Open Group, 'Identity Management', March 2004, available from: www.opengroup.org/idm/ • Crompton, M 'Proof of ID Required? Getting Identity Management Right', accessed 2008: www.privacy.gov.au/news/speeches/sp1_04p.html • Lee, S, 'An Introduction to Identity Management', SANS Reading Room, accessed 2008: www.sans.org/reading_room/whitepapers/authentication/852.php • ID Trust, Online Community, accessed 2008: http://idtrust.xml.org/ • Australian Legislation: Criminal Code Amendment (Theft, Fraud, Bribery & Related Offences) Act 2000 • Resources available on the AG's dept website: www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity

Focus area guideline 8: Identity management

Implementing technology controls

Information-centric technical controls

When implementing defence in depth in technology it is paramount to consider the value and type of information being protected as dictated by the defence in depth information-centricity principle. Doing so allows security mechanisms to be best positioned to protect the highest-value resources but also provide the greatest coverage.

In order to implement the defence in depth paradigm, the location and potential path of information assets must be understood. This allows various technical controls to be implemented to protect the information in layers 'permeating' out, both in storage and in transit.

This concept can be illustrated by applying it to an example scenario, where information is stored in a database on a system within a corporate network and accessed by a client application.

Example: Technology controls

At this point technical controls can be applied at the following levels:

- Application (database).
- Server host.
- Network.
- Client host.
- Client application.

By implementing controls at each of these levels, virtual overlapping protections can be created. This is illustrated by the following diagram, which shows an implementation of confidentiality controls in a typical client-server application scenario:

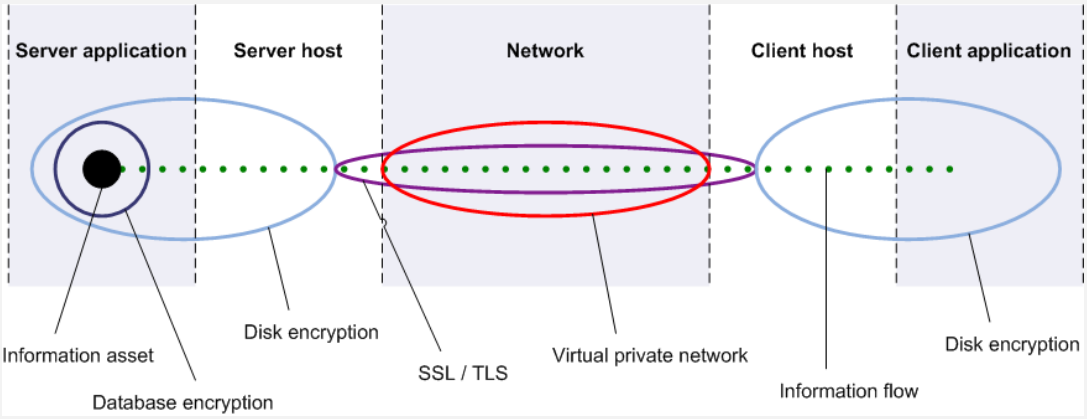


Figure 18: Sample technology information flow

Multi-use technical controls

Technology is able to provide overlapping protections in unrelated and separately developed and deployed controls. The overlap can take many forms including:

- **Information coverage**—controls are often general enough to be configurable across many information points and paths.
- **Attack lifecycle coverage**—technologies can often be configured to provide a combination of protection, detections, and response capabilities.
- **Security service coverage**—the confidentiality/availability/integrity triad is central to many technologies and in many circumstances requires only a configuration change to be enabled.

While separation, particularly functional separation, is often touted as a security benefit, it should be evaluated on a case-by-case basis to determine whether the coverage of extended overlap produces a greater benefit in terms of defence in depth.

Application (client and server)

Applications are the closest layer of defence to the actual information resources being protected and therefore are often also the last line of defence. Fortunately, applications, particularly custom applications, have the greatest scope for applying the strongest and most specific protections.

As the application security space (in particular the web application security) has matured over the past decade, many resources have become available for detailing the breadth of controls available[58,59,60,61,62]. Where commercial off-the-shelf applications are concerned, it is now somewhat standard for vendors to provide some security configuration documentation, in addition to the vast array of freely available community resources on the subject.

The following list provides a sample of technical controls that can increase application security:

- **Secure application design** in line with best-practice principles such as ‘least privilege’ and centralisation.
- **Strong authentication** using proven cryptographic techniques and where possible multiple ‘factors’.
- **Strong access control** applied consistently at every point of access (or every request).
  - **Auditing and logging** functionality to allow enable the detection of malicious activity and subsequent investigation.
  - **Password controls** to strengthen authentication in line with corporate password policy.
- **Input validation** applied consistently and holistically to prevent unauthorised access through malicious data injection.

[58] Open Web Application Security Project (OWASP), *OWASP Guide 2.1*, accessed 2008: http://www.owasp.org/
[59] Sivanandhan H, *Application Security Cheat Sheet*, accessed 2008: http://www.securitydocs.com/library/3387
[60] King S, *Applying application security standards - a case study*, *Computers & Security*, 2004, (23):17-21.
[61] Web Application Security Consortium, accessed 2008: http://www.webappsec.org/
[62] Howard M & Lipner S, *The Security Development Lifecycle*, Microsoft Press, 2006

- **Strong session management** based on standardised components.
- **Data encryption** using proven strong algorithms, such as the advanced encryption standard (AES).
- **Robust error handling** applied centrally to prevent undefined application states and the revelation of sensitive system information.
- **Accurate and complete documentation,** including security requirements and the mechanisms used to implement requirements.
- **Integrity checking** using strong cryptographic algorithms, such as SHA-256, to prevent data being modified or corrupted.
- **Security administration functions,** such as the disabling of user accounts, to enable efficient response to malicious activity.

Host (client and server)

Moving a step further away from where information is held leads to the host system. Traditionally the host has been an area of concentration for operational personnel. This is partly because there is a clear and well-defined trust boundary between the host and the rest of the network. That is, it is very easy to control information within a system but becomes difficult once it has left.

Trust boundary

The term 'trust boundary' refers to a physical or logical point where the trustworthiness of information changes. In general, trust boundaries are enforced through the validation of the correctness or appropriateness of information.

All modern operating systems vendors now publish hardening guides and other technical reference material. Additionally, the Center for Internet Security (CIS)[63] publishes benchmarks allowing technical staff to compare the level of security configured to industry-recognised best-practice standards. At the time of writing, benchmarks were available for major Microsoft operating systems and other leading Unix variants.

The following technical controls can be applied to both client and server systems depending on the required level of security:

- **Host intrusion detection** or file integrity monitoring to alert staff of compromise and maintain the integrity of data on the host.
- **Host intrusion prevention** to prevent attacks against a vulnerable system.
- **Host firewalling** to prevent services from being accessible to unauthorised parties.
- **Strong file permissions** to limit the impact of a successful compromise and even prevent some forms of attack that require access to restricted parts of the file system.
- **Strong program permissions** as a means of controlling programs, particularly client programs that have been taken over, and preventing them from accessing key system resources and information.

[63] www.cisecurity.org

- **Logging** of all security functions to a local and/or centralised location so attacks can be detected and reviewed.
- **Antivirus software** to protect against any malicious software or files that are uploaded or downloaded to the host.
- **Disk encryption** as a means of maintaining confidentiality of data.
- **Strong authentication** to ensure that only authorised personnel are connecting.

Network

The network and associated communications infrastructure also offers an opportunity to provide the greatest security coverage of information within an organisation, because in the vast majority of cases information must be communicated to be useful. As a result, the network can be exploited by organisations to provide the greatest level of security coverage through the implementation of controls at various information choke points.

While there are many technological controls that can form part of a defence in depth strategy throughout the network, and more are constantly being developed, the following list provides a sample of the most common controls:

- **Network intrusion detection** as a means of monitoring and identifying malicious activity throughout the network.
- **Network intrusion prevention** to prevent external exploits from reaching the internal network where they may be actualised.
- **Firewalls** to enforce communications policy at the perimeter and other internal choke points.
- **Network segregation** through routers, switches, firewalls and other devices.
- **Transport encryption** to prevent eavesdropping of sensitive data being transported across the network and internet.
- **Application firewalls/gateways** as a means of controlling application level traffic. These devices are fast becoming the most important choke points in the network.
- **Centralised authentication** to keep unauthorised users from accessing the network itself and also key resources and applications.
- **Denial of service protection** devices and services that help keep key information resources available to users.
- **Content filtering** to prevent malicious software from entering the network.
- **Centralised logging** to allow for easy incident analysis and establishment of consistent timelines across all available incident data.
- **Centralised key management.**

Control analysis

Specific controls in the area of information security processes for defence in depth include:

- Infrastructure security.
- Communications security.
- Network architecture security.
- Application security.

The following tables discuss these points in more detail.

Focus area guideline: Infrastructure security	
Description	Infrastructure security is the set of technical controls and business processes that determines infrastructure requirements for the delivery of business services and implements measures to protect systems and devices.
Objectives	• Identify infrastructure security requirements for delivery of services and user-applications • Implement secure data transmission, storage, protection and recovery • Implement effective maintenance policy and procedures • Provide physical security

Key controls	• Perimeter hardening and performance monitoring
	• System hardening
	  o Secure configuration (i.e. avoid default settings)
	  o Provide least functionality (i.e. restrict unnecessary services)
	• Filtering of infrastructure traffic
	• Cryptography
	  o Public key infrastructure
	  o Key management
	• Directory services
	  o Authentication infrastructure
	• Device patching processes
	  o Network devices
	  o Servers
	  o Desktops
	• Physical security
	  o Secure rooms for infrastructure (e.g. communications termination points)
	  o Restrict personnel access to servers/communications equipment
	• Fault tolerance/redundancy
	  o Business continuity planning (BCP)

Layered controls	• Infrastructure redundancy • Hardening of network devices, servers, desktops • Personnel access restrictions

Implementation	• Review existing infrastructure
	  o Inventory
	  o Network configuration/topology
	  o Communications system
	  o Redundancy capability
	• Assess infrastructure vulnerabilities
	• Configure infrastructure components to avoid common attacks
	  o Review vendor recommendations for device hardening
	  o Controlled configuration process
	• Implement required infrastructure changes

	o Configure the DMZ as an 'external' network o Provide support for the four-layered DiD network strategy o Identify vendor devices to improve DiD profile (e.g. unified threat management—UTM) • Address storage and transmission requirements o Security for network storage (e.g. SAN) o Sensitive information classification o Public key infrastructure (PCI) • Develop a standardised desktop strategy o Minimise desktop images—standard operating environment (SOE) o Disable non-essential services o Use security and compliance tools o Centralised desktop configuration management • Automated software distribution • Test the intranet, extranet, internet o Configure links for trusted partners o Packet filtering at router and proxy o Periodical and brute force testing • Control physical access o Develop and enforce access policy (layered controls) o Review vendor facilities (e.g. data centres) • Execute business continuity planning (BCP) o Data backup facility o Infrastructure requirements for development of BCP • Document administrative policy and procedures
Maintenance	• Review device configuration changes (i.e. who, why, when) • Monitor security forums for zero-day exploits • Monitor infrastructure for DoS attacks • Patch management processes and procedures o Conduct testing of new software releases/patches o Update device software (OS, application, firmware) • Harden security infrastructure in response to breaches • Change-control for new or decommissioned infrastructure • Audit desktop usage • Incident reporting
Further information	• Singh, K, 'IT infrastructure Security- Step by Step', SANS Reading Room, accessed 2008: www.sans.org/reading_room/whitepapers/basics/430.php • MacLeod, K, 'Patch Management and the Need for Metrics', SANS Reading Room, accessed 2008: www.sans.org/reading_room/whitepapers/bestprac/1461.php?portal=64384a0eca65a1c8ee0074505088851e • NIST Special Publication 800-53, 'Recommended Security Controls for Federal Information Systems', accessed 2008: http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-

	final-clean-sz.pdf ▪ Microsoft TechNet, 'Providing defence in depth for Your Desktop Deployment Projects', accessed 2008: www.microsoft.com/technet/community/columns/secmgmt/default.mspx

Focus area guideline 9: Infrastructure security

Focus area guideline: Communications Security	
Description	Communications security is the set of technical controls and business processes that determines the communications requirements for information and protects data against threats whilst in transit.

Objectives	• Protect communications against:
	  o Unauthorised access
	  o Eavesdropping
	  o Hijacking
	  o Impersonation attacks
	• Increase awareness of communications security risks
	• Comply with privacy legislation

Key controls	• Cryptographic methods
	  o Key management/public key infrastructure
	  o Transport layer
	  ▪ Transport layer security (TLS)
	  ▪ Secure sockets layer (SSL)
	  ▪ Internet protocol security (IPSec)
	  o Network layer
	  ▪ Virtual private network (VPN)
	  o Application layer (e.g. email)
	  ▪ Pretty good privacy (PGP)
	  ▪ Secure/multipurpose internet mail extensions (S/MIME)
	• Voice over IP (VoIP)
	  o Secure architecture, while maintaining quality of service (QoS)
	  o Authentication and access control for voice gateway
	  o VoIP-ready firewalls
	  o Isolation from PSTN
	• Third-party certification (e.g. VeriSign)
	• Secure communications awareness
	• Physical security measures for communications infrastructure

Layered controls	• Application of encryption across multiple network layers

Implementation	• Assess communications flows
	  o Develop a communications map
	• Identify mission critical communications
	  o Information sensitivity classification
	  o Develop communications policy for sensitive information transmission
	  o Identify trusted and untrusted communications links
	• Review privacy legislation and compliance requirements
	  o Resources available from the Office of the Privacy Commissioner
	• Select and implement communications encryption
	  o Identify communication channels requiring encryption
	  o Consult network architects for cryptographic implementation
	• Establish relationships with certification vendors for publicly accessible

	domains • Conduct training for personnel regarding the importance of secure communications (e.g. email encryption) o Provide documentation for communications policy and security methods • Define processes for mitigating communications breaches and potential brand-damaging media coverage
Maintenance	• Monitor for email anomalies • Enforce communications policy for sensitive information • Review risk profile for new communications technology • Respond to any enquiries from the Privacy Commissioner • Contain adverse public media by responding rapidly to communications breach
Further information	• Guidelines to Information Privacy Principles, accessed 2008: http://www.privacy.gov.au/government/guidelines/ • Xin, J, 'Security Issues and Coutermeasure for VoIP', SANS Reading Room, accessed 2008: http://www.sans.org/reading_room/whitepapers/voip/1701.php?portal=b4655a41dbc9852ceaa089807ff7ee9f • Defence Information Systems Agency, 'Draft Recommended Application Security Requirements, Version 2.0' accessed 2008: http://iase.disa.mil/stigs/stig/applicationsecurityrequirements.pdf • Axis Communications, 'Communication Security: available techniques', accessed 2008: http://www.axis.com/documentation/whitepaper/security.pdf • NSA, 'Information Assurance Technical Framework', 3.0, 2000

Focus area guideline 10: Communications security

Focus area guideline: Network architecture security	
Description	Network architecture security is the set of design controls and monitoring processes that protects information during processing, transmission and storage.
Objectives	• Protect information during processing, transmission and storage • Isolate public access from mission critical systems • Facilitate monitoring of network data for security incidents • Defend the end-user against malicious sources

Key controls	• Network segregation
	  o Trust zones and choke points
	  o Demilitarised zones (DMZs)
	  o Network Address Translation (NAT)
	  o VLANs
	  o Extranets and dedicated links
	  o Vendor variance
	• Data inspection
	  o Antivirus/anti-malware
	  o Content management/anti-spam
	• End-point security
	  o Data encryption
	  o Inbound and outbound access control
	  o Platform hardening
	• Intrusion detection
	  o Network intrusion detection (NIDS)
	  o Host intrusion detection (HIDS)
	• Logging and auditing
	  o Security event management and consolidation
	• Threat management
	  o Intrusion protection systems (IPS)
	  o Traffic management/bandwidth throttling
	  o Anti-virus (malware disinfection and/or quarantine)

Layered controls	• Inspection and control of data at all trust zones within the network • Implementation of varied protection/detection methodologies and technologies to ensure minimal ‘gaps’ • Isolation of unknown and untrusted data from critical systems • Reaction to malicious traffic

Implementation	• Allocate resources for architecture review
	  o Internal network security experts or external consultants
	• Review existing architecture
	  o Business units/operations
	  o Assess external vectors and threats (deductive and inductive)
	  o Identify network weaknesses using testing methodologies (perimeter, network, application, host)
	• Test network security

	◦ Penetration testing ◦ System testing • Implement network hardening ◦ Architecture modifications ◦ Firewalls ◦ Servers ◦ Desktops • Review external network connections ◦ Define trusted/untrusted sources ◦ Enforce security policy for all network connections • Document network architecture
Maintenance	• Monitor network ◦ Manual review of access logs ◦ Automated alerts (e.g. firewall, database access) ◦ Monitor for potential external and internal threats (e.g. media, security forums, personnel access logs) • Patch management • Update IDS signatures
Further information	• Straub, K, 'Information Security: Managing Risk with defence in depth', accessed 2008: http://www.sans.org/reading_room/whitepapers/infosec/1224.php • Ogren, E, 'Using a layered security approach to achieve network integrity', 2004: http://www.computerworld.com/printthis/2004/0,4814,89861,00.html • NIST Special Publication 800-27, 'Engineering Principles for Information Technology Security', 2001: http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf • US-CERT, 'Intruder Detection Checklist' http://www.us-cert.gov/reading_room/intruder_det_check.html

Focus area guideline 11: Network architecture security

Focus area guideline: Application security	
Description	Application security is the set of technical controls and business processes that determines application security risks and mitigates identified risks through secure development lifecycle processes.
Objectives	• Protect applications against security threats • Raise awareness of security requirements in application design, development, deployment and maintenance • Assess application security by conducting a vulnerability/threat analysis • Develop processes to foster secure application development

Key controls	• Developer awareness development and training
	• Secure application design
	• Authentication and authorisation
	• Auditing and logging
	• Password controls
	  o Aligned with access control policy
	• Input validation
	• Secure session management
	• Data encryption
	• Robust error handling
	• Documentation
	  o Secure application development
	  o Change control processes
	  o Standardised security testing tools and methodology

Layered controls	• Address application security during design • Isolation of software migration tasks • Data encryption • Access controls and authentication • Session management

Implementation	• Adopt secure application development and review processes
	  o Secure development guidelines for in-house and vendor engagements (SDLC)
	  o Conduct training for development personnel
	  o Best-practice processes/tools (OWASP, OASIS)
	  o Separation of tasks (e.g. for software migration)
	• Identify applications that support mission critical applications/services
	• Assess application vulnerability and threats
	  o Custom applications
	  o Off-the-shelf products
	  o Web applications
	  o Web services
	  o Mobile applications
	  o Monitor changes in the threat environment
	• Identify common vulnerabilities
	  o Injection attacks

	○ Buffer overflow ○ Scripting attacks • Identify and assess application-related components/configurations ○ Operating systems ○ Frameworks (e.g. J2EE, Net) ○ Databases ○ Firewalls (i.e. ports required to meet functionality) • Conduct application security assessment ○ Automated tools ○ Manual testing ○ Code reviews ○ Load testing ○ Assess adherence to security policy (e.g. access control requirements) • Document findings, conclusions and recommendations • Implement fixes to meet management's risk requirements
Maintenance	• Apply security patches and OS/framework updates • Develop and maintain security testing plan • Review and action security logs • Conduct security reviews for all subsequent development activities or application enhancements • Manage user accounts securely ○ Account revocation processes • Determine effectiveness of security measures through subsequent vulnerability assessment
Further information	• Open Web Application Security Project (OWASP), 'OWASP Guide 2.1', accessed 2008: www.owasp.org/ • Sivanandhan, H, 'Application Security Cheat Sheet', accessed 2008: www.securitydocs.com/library/3387 • Oasis Standard, 'Application Vulnerability Description Language (AVDL) v1.0 [OASIS 200403]', accessed 2008: www.oasis-open.org/specs/index.php • King, S, 'Applying application security standards- a case study', Computers & Security, 2004 (23):17-21. • Howard, Michael, Lipner, Steve, 'The Security Development Lifecycle', Microsoft Press, 2006 ▪ Web Application Security Consortium, accessed 2008: www.webappsec.org/

Focus area guideline 12: Application security

MONITOR AND REVIEW

The information security principles from the *Secure Your Information: Secure Your Business* paper relevant to this section are:

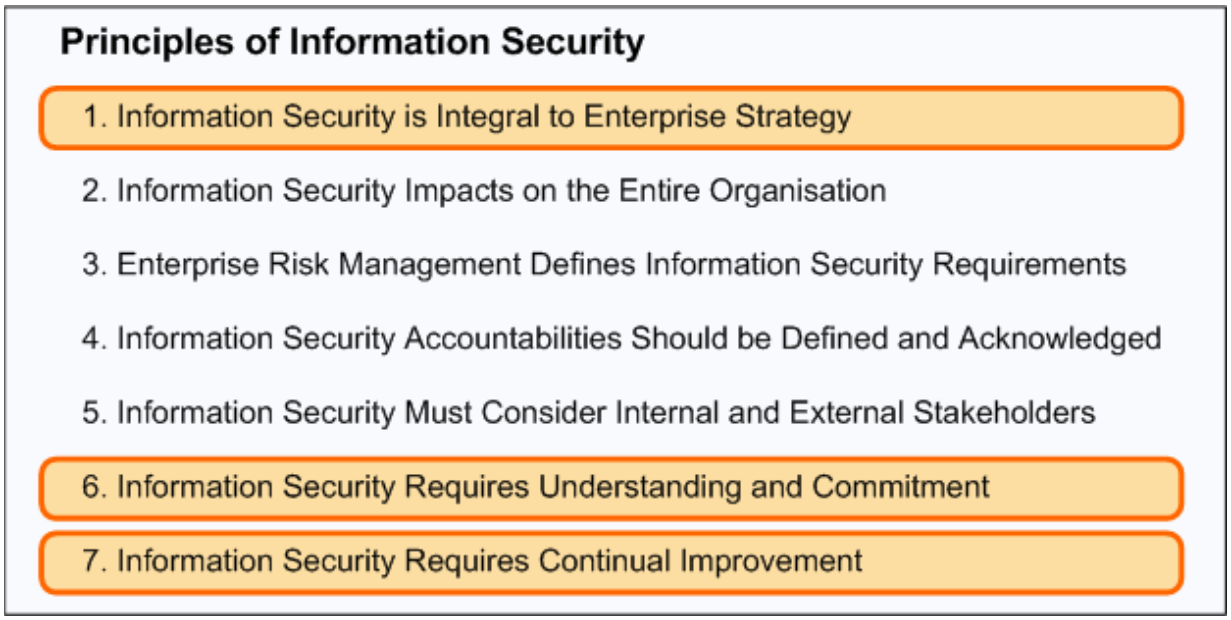


Figure19: Applicable principles of information security for monitor and review

The operational environment of today's organisations is dynamic: business objectives change as do the type of threats that exist in the external environment. The defence in depth strategy must adapt to these environmental changes in order to remain effective, and board-level support must be provided to facilitate ongoing monitoring and review.

Information security is critical for supporting the business mission and should be continually reviewed to address:

- security breaches and incidents
- weaknesses in existing controls
- changes in mission/business objectives
- changes in the security profile.

Corporate governance provides a framework for managing both organisational and environmental changes through policy enforcement.

Strategies for managing change

The corporate governance framework provides strategic direction and policy for managing both organisational and environmental change. Effective change management policies need to be available as part of effective governance and can be best addressed by considering *strategic change* and *operational change*.

Governance

Changes to organisational strategy can be driven by both internal and external factors. In order to assess the implications of strategic changes for the organisation's defence in depth approach, key actions include:

- ***Monitor environmental changes***—environmental changes (such as additional regulation or public opinion changing with regard to an industry sector) may require responses by the organisation's strategy in order to protect organisational assets and/or business processes. Training and special industry interest groups are valuable sources of information on the changing external environment.
- ***Maintain understanding of internal environment***—internal practices and organisational culture may require strategic changes to maintain a culture of security. Work habits, morale and contractual arrangements require ongoing awareness and assessment.
- ***Information sharing***—information sharing with service providers, industry regulators and interest groups allows organisations to maintain understanding of industry benchmarks and peer requirements for governance control.
- ***Define accountabilities***—staff accountabilities provide for ownership of information security responsibilities. By assigning accountabilities for information security management, organisational changes requiring realignment are significantly easier to identify and manage.
- ***Assess defence in depth performance***—the effectiveness of the organisation's information security framework requires ongoing performance monitoring to ensure the program is adequate in managing ongoing changes in the long term.
- ***Ensure currency of policies***—as tools which drive ongoing relevance, effective and concise policies must attempt to capture best-practice principles rather than detailing specific requirements. Policies, standards and procedures should attempt to maintain relevance to changing business operational requirements and introduction of new technology.
- ***Implement standards, procedures and guidelines***—policy statements should delegate detailed requirements to standards and procedure documents which are reviewed and developed on an annual basis to reflect changes in the work environment.

People

Operational change management provides assurance that infrastructure, network and system modifications are monitored, authorised, tested and documented[64]. Operational changes occur as a result of strategic changes or changes in underlying work practices or technology. Key actions within the area of operational change management include:

- ***Allocate roles and responsibilities***—the clear allocation of roles and responsibilities for operational change management is critical to enforce the relevant review required for change requests.

[64] Yarberry, W., *Effective Change Management: Ensuring Alignment of IT and Business Functions,* Information Security Systems, 2007,16:80-89

- ***Conduct training and awareness sessions***—annual or semi-annual training courses on information security are required for operational staff. Arming staff with knowledge for them to make the correct security decisions is crucial in a changing environment (e.g. the correct procedures for remote access). Awareness training programs should provide on-the-job examples as well as business justifications for why security is relevant to their specific role.
- ***Ensure security of third parties***—where outsourcing of business functions occurs, particularly when transfer, processing and storage of sensitive information is performed by the third party, imposing regular training and audit of the service provider's employees is essential to ensure their understanding of information security requirements.

Process

The following practices will assist organisations in achieving ongoing relevance of the processes which may affect the management of information security:

- ***Assess defence in depth effectiveness***—regular reviews of the effectiveness of the defence in depth framework should include review and assessment of all four elements of the defence in depth infrastructure (governance, people, process and technology). Where possible, metrics should be used to allow for objective comparison over time and between business areas.
- ***Develop incident response procedures***—standardised and effective procedures should be developed for emergency response items such as incident response and disaster recovery. These are of great importance as sudden changes may result in uncontrolled responses which may put information assets at significant risk.
- ***Standardise procedures to minimise uncontrolled changes***—standardised change request procedures in all areas of the business are to be reviewed by business owners to reduce the likelihood of uncontrolled changes. Furthermore, when changes are approved, the implementation should be scheduled to provide all stakeholders with knowledge of the change.

Technology

The following practices will assist organisations in achieving ongoing relevance of the technology structure in managing information security:

- ***Maintain awareness of new technologies and services***—a standardised selection process will ensure that a risk-based approach is taken to the evaluation of potential changes to the existing technology environment including the addition of new technologies and services.
- ***Track technical threats***—organisations should maintain knowledge of technical threats to the organisational environment and cross-reference to known vulnerabilities. Staff with roles in technology management can obtain such information via online forums and industry groups. Where vulnerabilities are released, their risks should be assessed and standard patching or configuration practices should be conducted.

Emerging challenges

Governance risks

Maintaining an effective and relevant information security governance program requires ongoing consideration for environmental changes. Recent challenges in this area have largely been a result of two factors:

- Changing regulatory environment.
- Evolving organisation design.

Changing regulatory environment

The regulatory environment for the governance of information security risks has dramatically changed over the past decade. Today, Australian Government legislation, vendor-specific requirements and industry regulations require the close attention of any information security manager. Recent and potential further changes in this area include:

- The introduction of data breach disclosure requirements in many jurisdictions around the world—since the introduction of such laws in the US State of California, the compromise of more than 200 million records containing personal or financial information has been publicised[65].
- Anti-money laundering/counter-terrorism financing (AML/CTF) legislation—for which December 2007 was the first significant deadline.
- The increased presence and enforcement of the Payment Card Industry—Data Security Standard (PCI-DSS)[66,67].

These changing regulatory requirements create a need to remain aware of the changing responsibilities organisations have for satisfying the requirements of both internal and external stakeholders.

Evolving organisation design

The evolving nature of organisational strategy and corresponding enterprise architecture presents additional challenges for the governance of information security. Consolidations and outsourcing arrangements have reshaped the need to have visibility and control over new and

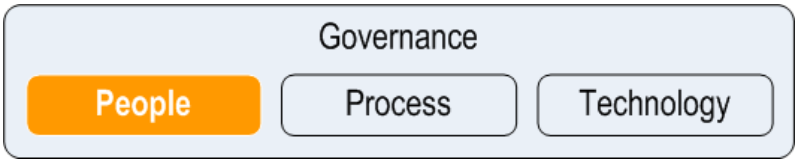
[65] ZDNet.com.au, *Top 10 security threats for 2008*, www.zdnet.com.au/news/security/soa/Top-10-security-threats-for-2008/0,130061744,339284653,00.htm
[66] ZDNet.com, *Top 7 security trends for 2008*, http://news.zdnet.com/2424-9595_22-177880.html
[67] *FAQ: What Visa's payment application security mandates mean*, www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9044323&source=rss_ind130

expanding organisational areas. The changing nature of the workforce and work arrangements has resulted in an erosion and expansion of the organisational perimeter.

Sustained skill shortages have resulted in an increasing interest in off-shoring arrangements. Australian organisations spent AU$22 billion on outsourcing arrangements in 2007[68].

Additional risks exist in an increasingly mobile workforce and the level of complexity is further compounded by contractors and vendors existing within the organisation's perimeter. In a recent study, 91 per cent of 381 UK and North American IT executives admitted that there was a greater risk of sensitive data being exposed to unauthorised persons when networks were accessible to remote workers and external users such as contractors. 89 per cent said there was a greater possibility of viruses while 85 per cent said there was a greater possibility of hacking in such workforce conditions[69].

People risks



Risks exist in the management of the human component of information security. Key challenges in this area are age-old risks:

- user understanding
- malicious insiders.

User understanding

User understanding of information security requirements remains a significant concern for organisations. The Deloitte Global Security Survey 2007 suggests that 79 per cent of respondents perceived information system failures to be a result of human error[35]. A significant challenge is the need to educate users, not only on the basics of information security principles, but also to keep them up to date with the latest user-facing threats.

In 2007, the shift in focus for hackers changed, with smaller numbers of users at a time being targeted (tens of thousands vs millions)[70]. Spear-phishing, or highly targeted phishing attacks, were highly publicised in 2007. Examples such as the Salesforce.com incident show that by gaining trust through legitimate identifiers gained through employee ID theft, fraudsters can derive substantial success.

SANS predicts that some of the key future attacks will be on web browsers, media players, instant messaging and peer-to-peer applications.

---

[68] Tung L, *2007: How was it for outsourcing?*, December 2007, www.zdnet.com.au/news/business/soa/2007-How-was-it-for-outsourcing-/0,139023166,339284584,00.htm
[69] King L, *Remote workers present 'security risk,' IT execs fear*, March 2008, www.computerworld.com.au/index.php/id;1784503569;fp;4;fpid;16
[70] *BusinessWeek*, 'Looming Online Security Threats in 2008', www.businessweek.com/technology/content/nov2007/tc2007119_234494.htm

Malicious insiders

A number of malicious user incidents impacted organisations in 2007. In the FBI/CSI Computer Crime and Security Survey, 64 per cent of respondent organisations experienced losses due to information security incidents as a result of insiders[71], and 90 per cent of respondents to the Deloitte Global Security Survey 2007 highlighted concerns about employee misconduct involving information systems[35].

Many organizations, including the SANS Institute, the CISSP/ISO 27000 Implementer's Forums, ZDNet and Computer Economics, are predicting a rise in the number of insider attacks in 2008[72]. These include technical threats from users abusing the access they are given and the threat of non-technical abuse of systems for fraud.

Process risks

Risk can also be embedded in the business process. These generally are a result of a changed environment (governance structure, people or technology) which removes the validity of an existing process. Key challenges in this area include:

- standardisation of processes
- authorisation bottlenecks.

Standardisation of processes

A key risk for organisations both large and small is the ongoing ability of their processes to respond to information security incidents that may arise. With factors such as the changing work environment and technology enhancements, organisations are struggling to maintain controlled practices which are uniform and tested.

By developing and maintaining a standardised process in advance of such an incident, the potential consequences of a breach can be minimised.

Authorisation bottlenecks

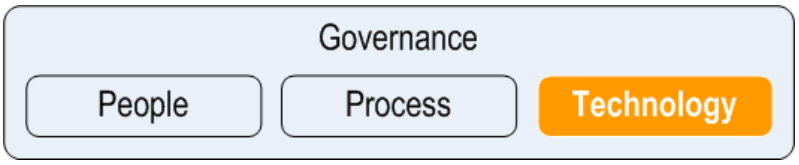
An additional risk to organisations is the existence of 'authorisation bottlenecks'. While it is good practice to ensure changes which materially impact on the organisation's architecture are managed through key decision-makers, organisations often place too much responsibility on a single authorisation entity.

As a result, the administration of such requests consumes a significant portion of management's time, removing its ability to achieve other strategic objectives. Furthermore, as

[71] FBI/CSI, *Computer Crime and Security Survey 2007*, www.gocsi.com
[72] CISSPforum/ISO27k Implementers' Forum, *Top Information Security Risks of 2008*, www.iso27001security.com/Top_information_security_risks_for_2008.pdf

the responsiveness to requests degrades, standardised processes become ineffective and may be ignored altogether.

Technology risks



As technology evolves, so do the various threats it faces. Recent challenges in the technology domain include:

- increased malware sophistication
- targeted application attacks
- convergence.

Increased malware sophistication

Malicious software, or malware, is neither a new concept nor a new challenge to security technology. However, as technologies and services have been achieving greater reliability and success in fighting traditional malware, malicious software authors have countered with increased sophistication.

For example, increased effectiveness of spam and malware filters for emails led to a drop in spam and malware propagation via email, with a corresponding increase in the use of websites to host the malware with emails including links to such sites. Furthermore, malware authors are migrating to technologies which are not as comprehensively serviced by effective security filters, such as private messaging systems, social and professional networking sites and instant messaging services.

Over the next year, security vendors expect to see new threats aimed at wireless transactional systems and users of less-sophisticated handheld hardware. It is predicted that mobile device attack development and execution will become more organised, moving towards use by criminal organisations.

Targeted application attacks

As commodity software, such as operating systems, web servers and remote administration packages, becomes more stable and mature, fewer vulnerabilities are being found and attackers are turning to custom software to find the path of least resistance. This is evidenced by the 2007 CSI/FBI Computer Crime and Security Survey[73] which reported that 33 per cent of organisations experienced targeted attacks, up from almost none the previous year. Targeted attacks on web applications are particularly on the rise.

Targeted attacks against custom applications present significant challenges as the technologies protecting them must include some level of custom code. Commercial off-the-shelf security

[73] http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

products alone are not enough because of the custom business logic present in target applications, as well as the need to protect against specifically crafted exploits that potentially bypass commodity protections.

Convergence

As the discipline of Enterprise Architecture has evolved, it has come under stronger and stronger influences from the forces of convergence. In particular, the technologies used within various architectures have been moving towards common platforms and components, most notably:

- applications have been simplified through the use of ubiquitous web interfaces
- voice and data networks have been integrated on flexible infrastructures
- multifunctional hand-held and network devices have become commonplace.

Converging technologies are challenging traditional security models in many ways:

- Devices and systems now perform functions in excess of business requirements and have become difficult to control, potentially resulting in abuse and unauthorised access.
- Overcrowded networks have even become single points of failure for mission-critical applications.
- Traffic and information assets crossing common infrastructure are now potentially exposed to blended threats both in terms of integrity and confidentiality.

APPENDICES

Appendix A: Glossary

BIA

A *business impact assessment* (BIA) is conducted as part of business continuity planning to determine the financial and operational impact of disruptive events on the business areas and processes of an organisation.

BPA

Business process analysis (BPA) is a methodology for the redesign of business processes to increase efficiency, improve customer support or reduce costs.

Botnet

A *botnet* is a network of compromised computers controlled by a malicious party, most commonly used to launch distributed denial-of-service attacks, or relay spam emails.

Convergence

In general, *convergence* is a coming together of two or more distinct entities or phenomena. Convergence is increasingly prevalent in the IT world. In this context the term refers to the combination of two or more different technologies in a single device. Taking pictures with a cell phone and surfing the Web on a television are two of the most common examples of this trend.

Defence in depth

Defence in depth is the coordinated use of multiple security countermeasures to protect an organisation's information assets.

ITSEAG

The IT Security group provides advice on technical solutions to problems identified by the nine Infrastructure Assurance Advisory Groups, as well as projecting emerging trends that have the potential to impact on all industry sectors.

ISO 27002

The ISO 27002 standard, formerly known as ISO 17799, is a set of established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organisation

LOPA

Layer of protection analysis (LOPA) is a methodology for hazard evaluation and risk assessment.

PCI DSS

The Payment *Card Industry Data Security Standard* (PCI DSS) is a comprehensive security standard intended to help organisations secure themselves against the threat of credit card fraud and identity theft. Organisations that process, store or transmit credit card numbers are required to comply with the PCI DSS standard.

Risk

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.

TISN

The *Trusted Information Sharing Network* (TISN) is a forum in which the owners and operators of critical infrastructure can work together by sharing information on security issues which affect critical infrastructure. The network is made up of a number of Infrastructure Assurance Advisory Groups (IAAGs) for different business sectors, and overseen by the Critical Infrastructure Advisory Council (CIAC).

Threat

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

Vulnerability

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

Vulnerability assessment program

A formal program which aims to describe and evaluate the vulnerabilities in an information system.

REFERENCES

1. US NSA, *Defense in Depth*, www.nsa.gov/snac/support/defenseindepth.pdf
2. TISN:*About Critical Infrastructure*, 2006, www.tisn.gov.au/
3. TISN, *Denial of Service/Distributed Denial of Service—Managing DoS Attacks*, 2006, www.dcita.gov.au/__data/assets/pdf_file/41312/DoS_Report.pdf
4. Grose S, '*Federal Government to Toughen Information Security*', ZDNet Australia, 2006, www.zdnet.com.au/news/security/soa/Federal-government-to-toughen-information-security/0,130061744,139249593,00.htm
5. Parker G, *The Military Revolution: Military Innovation and the Rise of the West 1500-1800*, Cambridge University Press 1996
6. Straub KR, *Information Security: Managing Risk with defence in depth*, August 2003, www.sans.org/reading_room/whitepapers/infosec/1224.php
7. Northcutt S, *Information Centric Approach to Defense in Depth*, February 2007, www.sans.edu/resources/securitylab/321.php
8. Australian Government, *Australian Government Information and Communications Technology Security Manual (ACSI 33)*, September 2007, www.dsd.gov.au/library/infosec/acsi33.html
9. Standards Australia, *AS 4360: Risk Management Standard*, 2004
10. Information Security Forum, *Business Impact Analysis*, June 2004, www.securityforum.org/assests/pdf/iram_assort.pdf
11. TISN, *Secure Your Information*, April 2007, www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~SIFT_Full_Report+020707.pdf/$file/SIFT_Full_Report+020707.pdf

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

13. Brooke P, *Building an In-Depth Defense*, Network Computing, 2001. www.networkcomputing.com/1214/1214ws1.html

14. Lewis JJ, About.com: *Grace Hopper Quotes*, 2005, womenshistory.about.com/od/quotes/a/grace_hopper.htm

15. Stevens J, *Information Asset Profiling*, June 2005, www.sei.cmu.edu/publications/documents/05.reports/05tn021/05tn021.html

16. OECD, *Guidelines for the Security of Information Systems and Networks*, July 2002

17. TeleTech, *Human Capital as a Force Multiplier*, January 2007, www.teletech.com/teletech/file/pdf/White%20Papers/HC_White_Paper.pdf

18. MI5 Security Service Report, *Personnel Security: Managing the Risk*—2nd edition, accessed 2008: www.cpni.gov.uk/Docs/Managing_the_Risk_2nd_edition.pdf

19. EPCONSULT, *Layer of Protection Analysis (LOPA)*, 2005, www.ep-consult.com/hazard_identification.shtml

20. Arkansas Department of Information Systems, *Policies/Standards/Best Practices*, 2005, www.dis.state.ar.us/poli_stan_bestpract/word/data_grid.doc

21. Robinson S, *Corporate Espionage 201*, 2007, www.sans.org/reading_room/whitepapers/engineering/512.php

22. US General Accounting Office, *Information Security Risk Assessment—Practices of Leading Organisations*, November 1999, www.gao.gov/special.pubs/ai00033.pdf

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

24. AusThink, *MECE—Mutually Exclusive*, November 2006, www.austhink.com/reason/tutorials/Tutorial_6/5_MECE_ME/mece_me.htm

25. Open Web Application Security Forum (OWASP), *Threat Risk Modelling*, March 2008, www.owasp.org/index.php/Threat_Risk_Modeling#DREAD

26. Standards Australia, *HB231 Information Security Risk Management Guidelines*, 2004

27. Standards Australia, *HB436 Risk Management Guidelines*, 2004

28. Tchankova, L, *Risk Identification—basic stage in Risk Management*, Environment Management and Health, 2002; 13(3):290-297.

29. Price L and Smith A, *Managing Cultural Assets from a Business Perspective*, accessed 2008: www.clir.org/pubs/reports/pub90/appendix1.html

30. Becker et al., *Guidelines for Business Process Modelling*, *Business Process Management*, 2000; 1806:241-261.

31. Information Systems Audit and Control Association (ISACA), *COBIT 4.1*, Monitor and Evaluate: Process Description, www.isaca.org

32. Castellanos et al, *Challenges in Business Process Analysis and Optimization*, Lecture Notes in Computer Science, 2006; 3811:1-10.

33. ITIL, *Information Technology Infrastructure Library (ITIL)*, www.itil-officialsite.com/

34. Minsky S, *The challenge of BPM Adoption*, accessed 2008: www.ebizq.net/topics/bpm/features/5757.html

35. Deloitte, *Global Security Survey 2007*, www.deloitte.com/dtt/cda/doc/content/ca_en_Global_Security_Survey.final.en.pdf

36. US NIST, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, sp 800-2, 2001: http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf

37. Open Web Application Security Project (OWASP), *OWASP Guide 2.1*, accessed 2008: www.owasp.org/

38. Sivanandhan H, *Application Security Cheat Sheet*, accessed 2008: www.securitydocs.com/library/3387

39. Warren P and Davies N, *Managing the risks from information- through semantic information management*, BT Technology Journal, 2007; 25(1):178-191

40. Knight K, *Resolving Challenges to Implementing Risk Management*, accessed 2008: www.tbs-sct.gc.ca/rm-gr/international/pp/challngs-%E9cueils_e.asp

41. US NSA, *Information Systems Security Engineering*, accessed 2008: www.nsa.gov/ia/government/isse.cfm?MenuID=10.3.2

42. Robinson D. *Defense in Depth: A Small University Takes Up the Challenge, SANS, Case Studies*, 2002. www.sans.org/reading_room/whitepapers/casestudies/710.php

43. Brooke P, *Building an In-Depth Defense, Network Computing*, 2001. www.networkcomputing.com/1214/1214ws1.html

44. Republique Francaise Premier Ministre, *In Depth Defence applied to Information Systems: Memo*, www.ssi.gouv.fr/en/confidence/documents/methods/mementodep-V1.1_en.pdf

45. US NIST, *Information Security Handbook: A Guide for Managers sp800-100*, 2006, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

46. Mark R, *Humans Still Weakest Security Link*, 9 Jun 2004, Internet News, www.internetnews.com/security/article.php/3366211

47. Bolman and Deal, *Reframing Organizations*, 2003, Jossey-Bass

48. *Leading Practices and Guidelines for Enterprise Security Governance* , 2006, www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~IT+Security+&+Governance.pdf/$file/IT+Security+&+Governance.pdf

49. Birkbeck *University of London, Human Resources—Network Security Policy*, 2006, www.bbk.ac.uk/hr/policies_services/policies_az/networksecurity

50. Nolan J, *Best Practices for Establishing an Effective Workplace Policy for Acceptable Computer Usage*, 2005, Information Systems Control Journal

51. Robb D, *Protecting Sensitive Data Requires Vigilance: HR and IT Should Work Together To Safeguard Systems From Internal and External Threats, 2002*, HR Magazine, http://search.looksmart.com/p/articles/mi_m3495/is_4_47/ai_84928073

52. ISO, *ISO 27002: 2005, Information technology - Security techniques - Code of practice for information security management*, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

53. Standards Australia, *New Security Standards Help Protect Community*, www.standards.org.au/downloads/060719_New_security_standards_launched.pdf

54. CompTIA, *Summary of Information Security: A CompTIA Analysis of IT Security and the Workforce*, CompTIA Research, 2007, www.comptia.org/sections/research/reports/200704-ITSecurity.aspx

55. Coe K, *Closing the Security Gap*, August 2003, HR Magazine, www.shrm.org/hrmagazine/articles/0803/0803coe.asp

56. Mendham T, *A Secure Culture*, February/March 2006, CIO Enterprise Focus: Security

57. Ross E, *Sack With Care*, 25 January 2006, Business Review Weekly

58. ISO, *ISO 27002: 2005, Information technology - Security techniques - Code of practice for information security management*, www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

59. Open Web Application Security Project (OWASP), *OWASP Guide 2.1*, accessed 2008: www.owasp.org/

60. Sivanandhan H, *Application Security Cheat Sheet*, accessed 2008: www.securitydocs.com/library/3387

61. King S, *Applying application security standards - a case study*, Computers & Security, 2004 (23):17-21.

62. Web Application Security Consortium, accessed 2008: www.webappsec.org/

63. Howard M & Lipner S, *The Security Development Lifecycle*, Microsoft Press, 2006

64. Yarberry, W., *Effective Change Management: Ensuring Alignment of IT and Business Functions, Information Security Systems*, 2007:16:80-89

65. ZDNet.com.au, *Top 10 security threats for 2008*, www.zdnet.com.au/news/security/soa/Top-10-security-threats-for-2008/0,130061744,339284653,00.htm

66. http://www.cisecurity.org/

67. ZDNet.com, *Top 7 security trends for 2008*, http://news.zdnet.com/2424-9595_22-177880.html

68. FAQ: *What Visa's payment application security mandates mean*, www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9044323&source=rss_ind130

69. Tung L, 2007: *How was it for outsourcing?*, December 2007, www.zdnet.com.au/news/business/soa/2007-How-was-it-for-outsourcing-/0,139023166,339284584,00.htm

70. King L, *Remote workers present 'security risk,' IT execs fear*, March 2008, www.computerworld.com.au/index.php/id;1784503569;fp;4;fpid;16

71. BusinessWeek, *Looming Online Security Threats in 2008*, www.businessweek.com/technology/content/nov2007/tc2007119_234494.htm

72. FBI/CSI, *Computer Crime and Security Survey 2007*, www.gocsi.com/

73. CISSPforum/ISO27k Implementers' Forum, *Top Information Security Risks of 2008*, www.iso27001security.com/Top_information_security_risks_for_2008.pdf

74. FBI/CSI, *Computer Crime and Security Survey 2007*, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf

75. CISSPforum/ISO27k Implementers' Forum, *Top Information Security Risks of 2008*, www.iso27001security.com/Top_information_security_risks_for_2008.pdf

76. FBI/CSI, *Computer Crime and Security Survey 2007*, http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf