



**Australian Government**

---

**Department of Communications,  
Information Technology and the Arts**

## **Managing IT Security**

### **When Outsourcing to an IT Service Provider:**

### **Guide for Owners and Operators of Critical Infrastructure**

**May 2007**



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

**DISCLAIMER:** To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgment of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

## Foreword

Managing Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure (guide) is designed to help managers to identify and address IT security issues when organisations are negotiating new, or renegotiating existing outsourcing contracts for their IT arrangements.

The guide has been prepared by the Department of Communications, Information Technology and the Arts (DCITA) on behalf of the IT Security Expert Advisory Group (ITSEAG)<sup>1</sup> of the Trusted Information Sharing Network (TISN)<sup>2</sup>.

The guide is based on a document released by the former National Infrastructure Security Coordination Centre in the United Kingdom (UK) (now known as the Centre for the Protection of Critical Infrastructure) entitled, 'Outsourcing: Security Governance Framework for IT Managed Service Provision'<sup>3</sup>. DCITA would like to thank the UK Government for allowing the Australian Government to draw on this resource. DCITA would also like to thank DLA Phillips Fox who provided advice in relation to the Australian legal and regulatory environment.

This guide is not intended to replace established information security standards issued by industry bodies. Organisations should also continue to seek appropriate legal advice to ensure that any IT outsourcing contract sets out in detail, and in a legally enforceable manner, the security requirements and outcomes identified by the organisation.

A shorter version of this document has been prepared for Chief Executive Officers and Senior Executives<sup>4</sup>.

### Critical Infrastructure Security

Infrastructure and Security

ITSEAG Secretariat

Department of Communications, Information Technology and the Arts

Email: [itseag@dcita.gov.au](mailto:itseag@dcita.gov.au)

Web: [www.dcita.gov.au/](http://www.dcita.gov.au/)

[www.tisn.gov.au](http://www.tisn.gov.au)

---

<sup>1</sup> The ITSEAG is one of several Expert Advisory Groups established within the Trusted Sharing Information Network for Critical Infrastructure Protection. The ITSEAG provides advice to the Critical Infrastructure Advisory Council (CIAC) and the sector based Information Assurance Advisory Groups (IAAGs) on IT security issues as they relate to critical infrastructure protection. The ITSEAG membership consists of academic specialists, vendors, consultants and some industry association representatives who are leaders in the information technology/e-security fields.

<sup>2</sup> TISN enables the owners and operators of critical infrastructure to share information on important issues. It is made up of a number of sector-specific Infrastructure Assurance Advisory Groups (IAAG), several Expert Advisory Groups (EAGs), and the Critical Infrastructure Advisory Council (CIAC—the peak body of TISN that oversees the IAAGs and EAGs). More on TISN can be sought from [www.tisn.gov.au](http://www.tisn.gov.au) or by contacting [cip@ag.gov.au](mailto:cip@ag.gov.au).

<sup>3</sup> Available at [www.cpni.gov.uk/Products/guidelines.aspx](http://www.cpni.gov.uk/Products/guidelines.aspx)

<sup>4</sup> Available at [www.tisn.gov.au](http://www.tisn.gov.au)

## Table of contents

Executive summary .....	4
1. Issues in outsourcing information security .....	7
1.1. IT security governance and outsourcing .....	7
1.2. IT governance: the relationship to critical infrastructure .....	8
1.3. Information security issues preceding an outsourcing arrangement .....	8
1.4. Potential IT security pitfalls associated with IT outsourcing .....	11
2. Managing IT security when outsourcing IT functions .....	13
2.1. Your organisation's and your service provider's responsibilities .....	13
2.2. Effectively managing security in the outsourcing process .....	16
2.3. Risk assessments .....	17
2.4. Transitional arrangements .....	19
2.5. Issues to be addressed in the contract .....	19
3. Resources .....	24
Attachment A Regulatory and Risk Environment .....	25
Attachment B Security Requirements, Communication, Management and Assurance Approaches .....	28
Attachment C Key Elements and Tasks—Outsourcing and Information Security .....	32

## Executive summary

This guide provides resources and checklists to assist managers to address IT security issues when organisations are negotiating new, or renegotiating existing outsourcing contracts for their IT arrangements. The ITSEAG has released a guide to effective IT security governance which should be seen as a companion to this guide.

This guide is not intended to be a stand-alone resource, and should be read in conjunction with the resources listed in Section 3 for further details as to specific requirements, in addition to obtaining independent legal advice as to regulatory compliance necessary for particular industry sectors.

Outsourcing an organisation's IT functions is a complex process to manage with IT security one of the many elements that needs to be considered.

This guide includes advice on:

- IT security issues to consider in the lead up to implementing an IT outsourcing arrangement;
- steps which need to be taken before and during negotiation and preparation of IT outsourcing contracts;
- a checklist of potential IT security pitfalls associated with IT outsourcing;
- advice on how to put in place effective IT security arrangements between an organisation and the IT service provider; and
- ideas on how to implement effective contractual arrangements and make them adaptive to changes in the IT security environment.

Good IT security governance is an essential part of an overall corporate governance strategy—particularly when considering outsourcing part, or all of an organisation's IT functions. Ultimately, in the event of a significant incident involving an organisation's IT, it is the organisation's bottom-line and reputation that will be effected by disruptions caused by IT failure or the loss of confidential information. The consequences of failure, particularly for organisations dealing with critical infrastructure, can also have widespread national-security and social implications, and cause considerable economic disruption.

The *Corporations Act 2001* imposes a number of legal responsibilities upon company directors, secretaries and officers and suggests an obligation to uphold due care and diligence<sup>5</sup>. Depending on the agreed terms of the contract, outsourcing transfers varying levels of management control, but it does not transfer compliance responsibility. Companies need to be aware that outsourcing IT functions to a service provider does not absolve a company, or its senior management, from its legal obligation to provide secure IT arrangements. In addition, government entities will not be absolved from any other obligations within government to comply with and implement government policies and procedures.

In Section 1, the guide outlines pre-outsourcing IT security considerations and examines the consequences of failing to implement stringent risk mitigation strategies during the outsourcing process and contract negotiation.

---

<sup>5</sup> *Leading Practices and Guidelines for Enterprise Security Governance*, TISN, June 2006, p 43  
[www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications](http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications)

The potential consequences include loss of revenue, loss of market credibility and a resultant fall in the share price, and exposure to litigation (both corporate and personal). Critical infrastructure providers should note that they are particularly susceptible to class actions if disruptions to service provision or the operation of critical infrastructure causes interruption to the broader economy. In addition, the introduction of 'corporate culture' offences under the Commonwealth Criminal Code has created a new basis for potential liability in the outsourcing context. If a critical infrastructure provider fails to 'maintain a culture of compliance with Commonwealth laws', the provider itself can be held liable for a breach of those laws by its employees or contractors (including, in this context, the outsource contractor). Maintaining a culture of compliance will include ensuring that the critical infrastructure provider's information security practices and processes comply with all applicable Commonwealth legislation.

Section 1 also examines some of the pitfalls that could potentially befall an organisation in an IT outsourcing arrangement. These include:

- the assumption that service providers will implement best-practice security, when in fact service providers are only obliged to implement what they have been contracted (and paid) to do; and
- failure to define and enforce stringent security requirements and enforce an obligation for service providers and their subcontractors to perform against these requirements in each IT outsourcing contract.

Section 2 of the guide examines the management of security in the contracting lifecycle.

In Section 2, the guide also suggests the need to have people on-hand with suitable expertise to ensure that:

- the outsourcing contract is going to be properly managed throughout its lifecycle;
- appropriate monitoring and reporting as well as auditing procedures are being adhered to; and
- if something does go wrong, incident management strategies are in place and staff know what to do.

Establishing key roles and making staff aware of their responsibilities (and knowing those of the service provider) will go a long way to building a culture of IT security.

This guide also provides additional tools to help implement an Information Security Management System (ISMS) internally, before outsourcing, and between your organisation and your IT service provider. An ISMS is an approach to IT security management which ensures that accountability for information security rests at the appropriate seniority level, that ongoing training and information are provided to employees and others, and that reasonable steps have been taken to ensure information security in light of:

- the organisation's resources;
- the organisation's risk profile and likely severity of harm to be sustained; and
- the regulatory obligations applicable to the particular organisation.

A suitable ISMS can also assist in managing the relationship between your organisation and the service provider and its subcontractors, and ensure the flow of information concerning risk assessment, security requirements, reporting, security assurance, and right of audit is managed throughout the contract lifecycle.

# 1. Issues in outsourcing information security

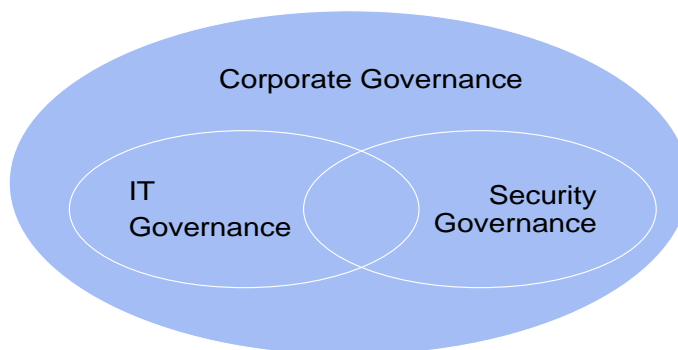
Your organisation is responsible for its IT security in any IT outsourcing arrangement. An organisation cannot effectively achieve IT security objectives without a strong and effective security governance framework. The ITSEAG has released a guide to effective IT security governance which should be seen as a companion to this guide.

## 1.1. IT security governance and outsourcing

Outsourcing can be seen as a business or commercial strategy pursued to achieve the strategic goals of an organisation. Drivers may include cost savings, increased business flexibility, exploitation of new technologies and accessing specialist expertise. No matter what the drivers are for outsourcing, if IT security is not properly considered, an incident involving your IT functions caused by human error, systems failure, or even malicious code could end up negating any net benefits derived from the outsourcing arrangement.

Organisations should view IT security governance as a significant component of an overall IT outsourcing model. Given the role information and IT systems now play in the core operations of organisations, IT security governance is now a key element of good corporate governance.

Figure 1—Corporate, IT and security governance relationships<sup>6</sup>



The broad stages which require consideration in ensuring information security in outsourcing arrangements are as follows (more detail is provided in Attachment C):

1. Ensure appropriate internal information security management system (ISMS) in place;
2. Identification, assessment and evaluation of risks;
3. Procurement security steps;
4. Roles and responsibilities;
5. Contracting for information security;
6. Transitional security arrangements;
7. Assurance and conformance;

---

<sup>6</sup> *Leading Practices and Guidelines for Enterprise Security Governance*, TISN, June 2006, p 1  
[www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications](http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications)

8. Ongoing security management (including change management);
9. Incident management and reporting; and
10. Termination and transition.

Although you may have internal IT and security governance systems in place, it is possible that your IT and security governance policies may not have been designed for an outsourcing arrangement where the roles and responsibilities are shared between your organisation and a new service provider (Section 1.3).

Your IT security governance policies, both internal and external, should be firmly based on an understanding of potential threats (including those of potential outsourcing pitfalls) to your organisation, legislative and regulatory compliance obligations and be underpinned by risk assessments, incident management strategies and testing.

It is important to make a distinction between IT security governance and IT security management. IT security governance sets the tone from the top down for implementing a culture of accountability and is used to ensure that all security management functions are designed and properly implemented. IT security management, on the other hand, is more a method of delivering IT systems in accordance with governance principles. Section 2.2 discusses a model for information security management.

## **1.2. IT governance: the relationship to critical infrastructure**

Good IT security governance is even more critical, and the consequences of disruption more severe, if you are an owner or operator of critical infrastructure.

The Australian Government defines critical infrastructure as:

“...those physical facilities, supply chains, information technologies and communication networks which, 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.”<sup>7</sup>

Information Communication Technologies (ICTs) are now an indispensable feature of the modern economy and, therefore, inextricably linked with critical infrastructure. In such an environment, the consequences of poor IT governance and subsequent IT failure can have widespread flow-on effects.

## **1.3. Information security issues preceding an outsourcing arrangement**

Prior to entering into an IT outsourcing arrangement, care should be taken to ensure that any internally developed policies, standards and compliance requirements are sound and that they are regularly reviewed. This is important, because if poorly conceived, they could find their way into IT outsourcing arrangements and significantly distort and disrupt IT security compliance.

---

<sup>7</sup> *Critical Infrastructure Protection: Whose responsibility is it?*  
[www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications](http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications)

An organisation needs to be confident that it has the in-house expertise to profile risk for its IT security and the capability to manage and review the IT security functions it intends to outsource. If an organisation lacks capability in these areas, it is unlikely to be able to design an outsourcing contract that ensures that the outsourced IT security functions are properly managed by the service provider. During the earlier stages of planning the outsourcing contract, your organisation should determine whether it has the in-house capability to effectively manage its IT security or whether it would be better to outsource IT security management to a qualified third party.

This guide is based on the premise that you have decided to outsource part, or all of your IT functions, and that outsourced functions will be brought under the umbrella of your organisation's IT security governance policies and strategies.

Before you start the outsourcing process, it is suggested that you run through a quick 'check list' of information security issues to make sure that your IT security governance and procedures will have sufficient security, staffing and reporting mechanisms in place to effectively ensure information security and protect your IT functions. It is possibly too late, or will involve a significant, resource-intensive effort to vary an outsourcing arrangement, once a contract is in place. Figure 2 provides a checklist of some issues that you should consider.

Figure 2—Information security issues checklist

### **Information Security Requirements**



System and communication security standards to be met by both provider and the organisation's systems



Protection of confidential information and intellectual property of the organisation



Protection of personal information and client data



Compliance with information, security and privacy policies, laws and regulations



Removal of data from redundant systems and any leased systems



### **Internal & External Staffing Considerations**

Employment of appropriately qualified and experienced staff and information security managers



Details of staff and contractor supervision



Security clearance, staff checks and police checks as appropriate



Access Protocols and remote access controls to be met by the provider, its staff and contractors



Supervision, monitoring, security clearance and control of, and responsibility for, subcontractors



Indemnity provisions to be provided by provider and its contractors



### **Accountability, Reporting & Compliance Considerations**

System security requirements and compliance



Security reviews and security audits



Reporting security breaches



Disaster recovery, evidence retention protocols and reporting policy



Business continuity plans—your own and the provider's



Security incident and risk management and reporting obligations



### **Contract Transition/Termination**

A clear contractual arrangement for the termination/transition process



A clear understanding by the organisation and the service provider of the



termination process

#### **1.4. Potential IT security pitfalls associated with IT outsourcing**

Outsourcing your organisation's IT functions while maintaining IT security is a complex process, and cannot be dealt with in a simplistic way. A number of IT outsourcing pitfalls of which you should be aware when drafting and negotiating the outsourcing contract are detailed below:

When your organisation:

- is unaware of the security risks and regulatory compliance obligations involved, in terms of the business impact of IT failure, the threats to the IT systems, and their current vulnerabilities;
- does not make service providers aware of the security risks and regulatory compliance obligations relating to the business areas and IT systems being outsourced;
- assumes that service providers will implement best-practice security, when they may only implement what they have been contracted (and paid) to do;
- assumes that IT security is inferred as part of functionality requirements, when requirements for security need to be explicitly specified;
- specifies draft, imprecise or inconsistent policies or security standards to be complied with, or refers to standards or codes of practice which allow considerable variance in interpretation;
- is unaware of changes to the risk and/or regulatory landscape due to the continually changing e-security environment;
- signs up to levels of security which were in place at the time of transitioning, and are subsequently surprised by scope-changes as the e-security environment changes;
- tries to micro-manage and specify security requirements with such detail that the service provider has little room for innovation or flexibility;
- continues to manage IT security at the detailed level, even though the intent was that the work should be outsourced, thereby duplicating effort and confusing accountabilities;
- fails to continually monitor its information networks for intrusions or suspicious activity and have in place incident response plans, or fails to engage in appropriate testing.

When your organisation's management:

- tacitly permits reductions in IT security, functionality or service level when they are not measured or accountable for them;
- is unaware of the risks of potential criminal and/or civil liability; and
- do not consider themselves accountable for security when IT functions are outsourced.

When your organisation's outsourcing contract:

- aims to over-simplify IT security requirements into contract clauses, such that the resulting measures may be inadequate in countering risk;
- does not have the flexibility to accommodate changes to the your business' risk environment;
- fails to define security requirements, meaning that the service provider is not obliged to implement or operate required measures; and
- fails to articulate transition requirements from one service provider to the next, or termination arrangements.

When your service provider:

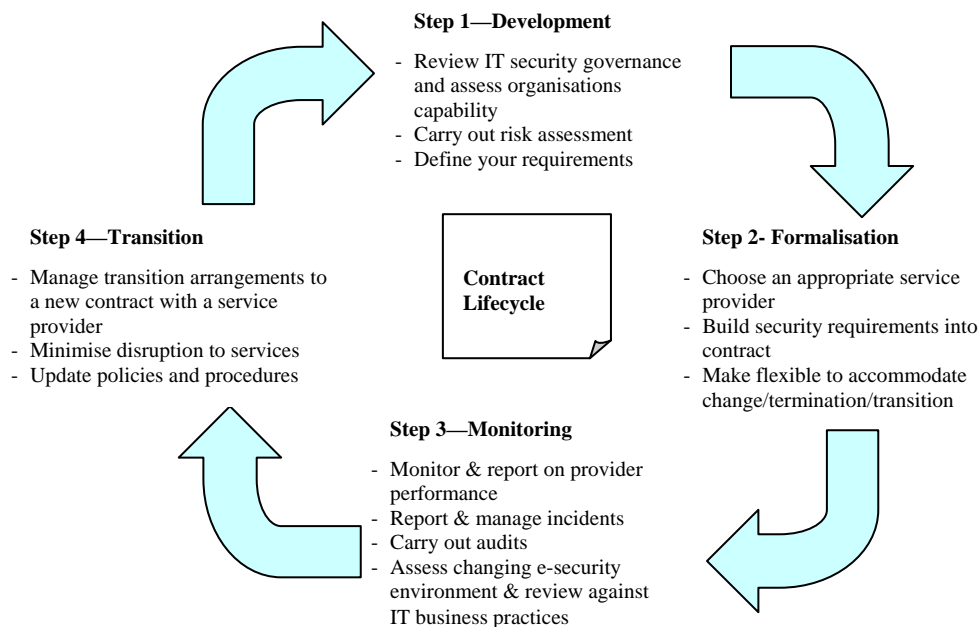
- and its commercial directors and service delivery managers do not consider themselves to be accountable for IT security as a key part of your organisation's contract;
- fails to allocate sufficiently skilled, experienced and qualified resources to security management;
- cuts back on security processes which are not explicitly set out in the contract in order to meet cost-savings targets or increase contract margin performance and, as a result, key security elements such as patch management, intrusion detection, monitoring, and secure system design and build processes do not happen;
- seeks any opportunity to reduce costs and increase margin, including further subcontracting of services unless the contract prohibits it;
- resists your organisation's attempts to gain visibility of IT security processes, or to commission assurance reviews or audits of security;
- provides assurances which fail to meet your organisation's requirements;
- deals with post-contract requirements for security improvement as material scope extensions, sometimes considerably increasing charges (often inflated commercially by considerable scope-change margins) to the organisation;
- resists requirements to change security measures once contracts are signed if they consider that such changes are commercially unattractive to them; and
- without your awareness and/or agreement, further subcontracts elements of their service delivery to a third party outside the Australian legal and regulatory framework, which may not offer adequate IT security safeguards.

## 2. Managing IT security when outsourcing IT functions

Any approach to dealing with information security risks should be founded in an organisation-wide strategic plan, starting with the organisation's overall IT strategy. The overall strategic plan should then inform management of the IT security aspects in each outsourcing arrangement. This will enhance consistency between outsourcing arrangements and the enterprise-wide strategy, make administration more efficient, increase the likelihood of compliance, and allow for easier detection of systemic and organisational issues.

Figure 3 illustrates important on-going IT security issues which become relevant at different stages in the contract life-cycle, and which should be considered during the planning stage and execution of your IT outsourcing arrangements.

Figure 3—Security in the contracting life-cycle



### 2.1. Your organisation's and your service provider's responsibilities

Your organisation is responsible for ensuring the security of its assets and must accept that security is a valid business cost. While it is not possible to secure all critical infrastructure from all threats, good business practices, such as applying risk management techniques to your planning processes, conducting regular reviews of regulatory framework, risk assessments and plans, and developing and reviewing business continuity plans, will help your organisation to mitigate potential risks and threats.

When outsourcing, there are a number of key responsibilities to be established within your organisation and with the successful bidder. Contracts should establish key IT security roles and responsibilities within your organisation and service provider organisations. Figure 4 is a hierarchical diagram illustrating the responsibilities of key

personnel in your organisation in an IT outsourcing arrangement. Similarly, Figure 5 examines the key roles and responsibilities in your service provider’s organisation.

*Figure 4—Key responsibilities of key personnel in your organisation*

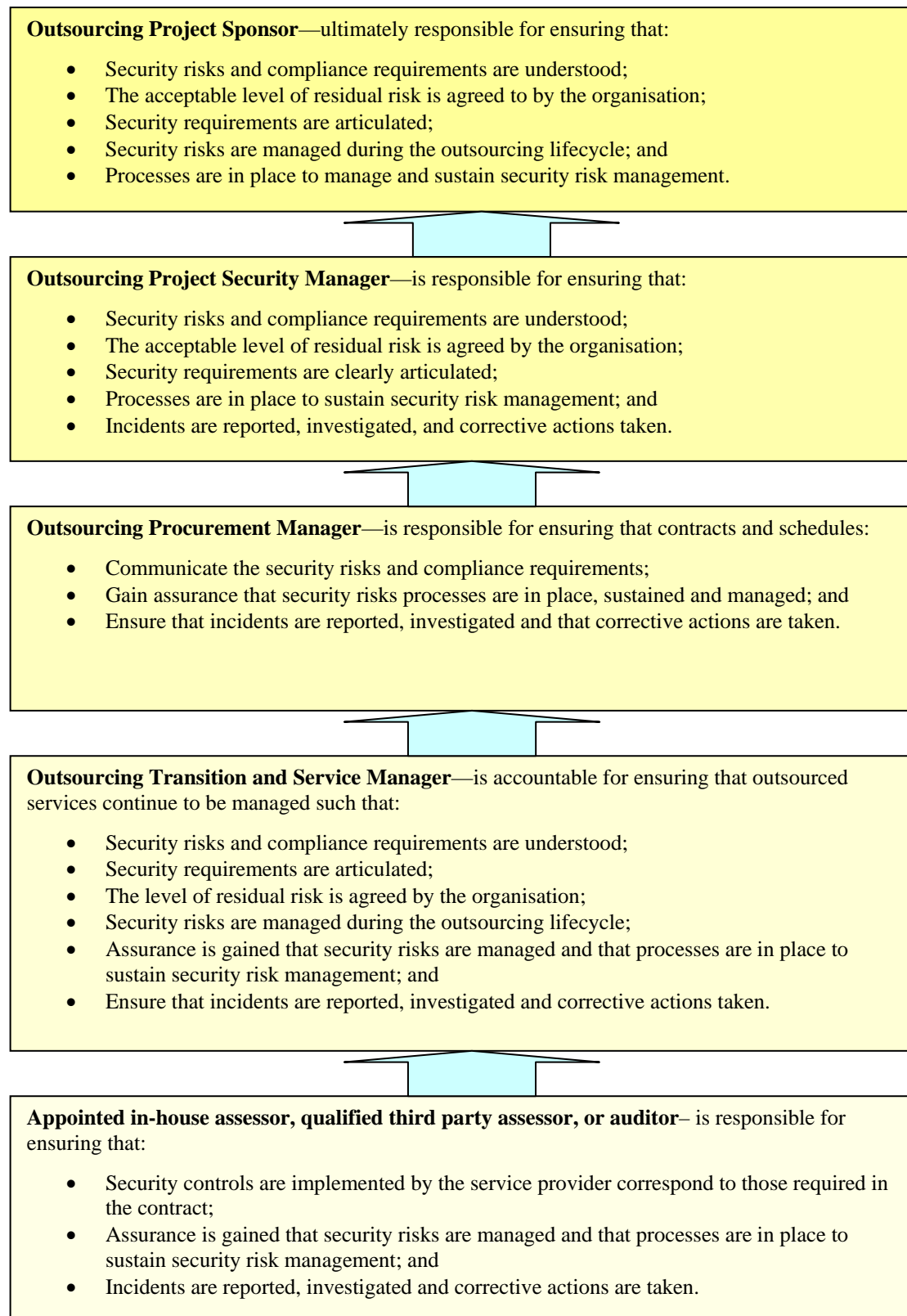
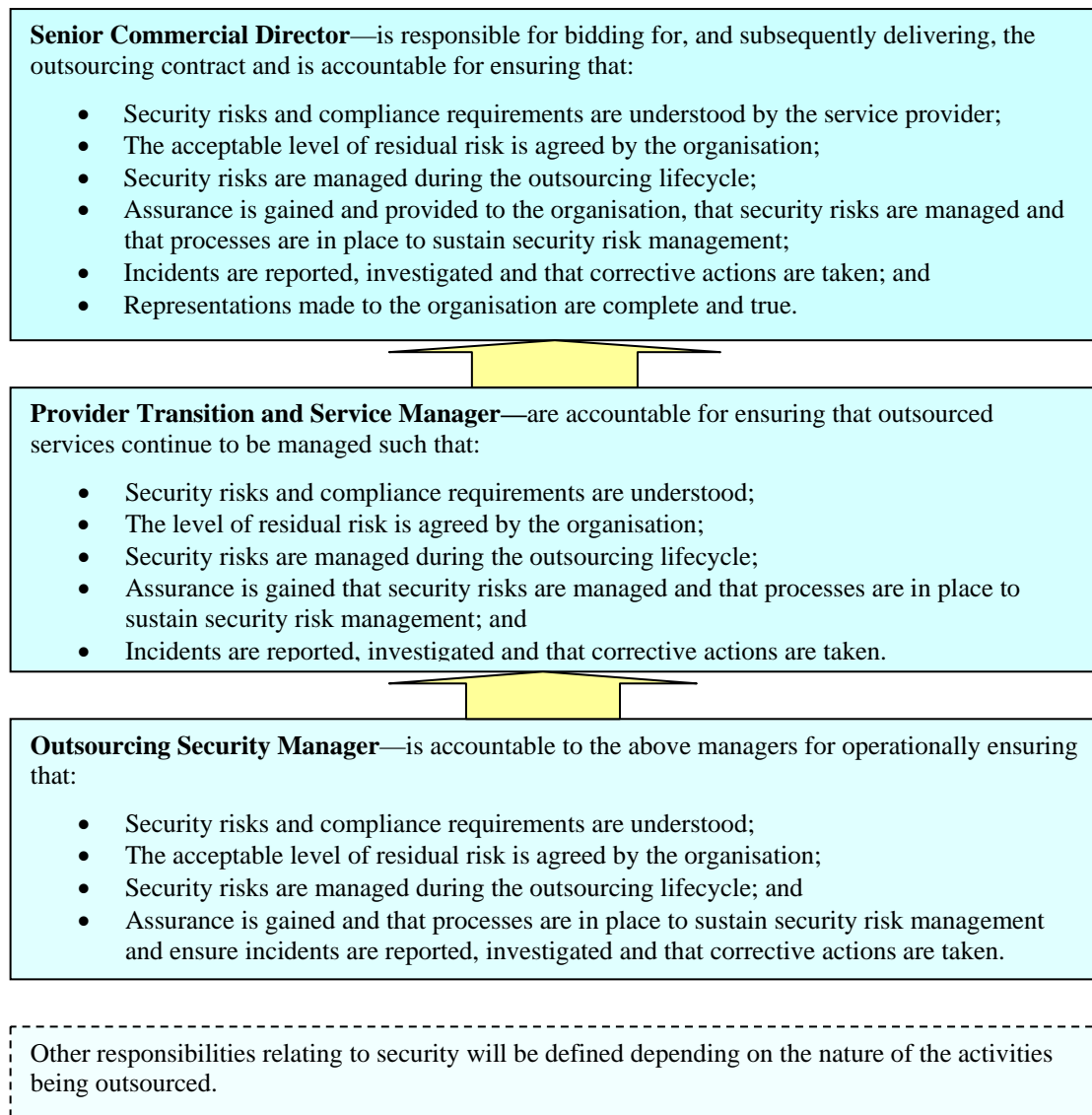


Figure 5—Responsibilities of key personnel in your service provider’s organisation



### 2.1.1. Liability and compliance issues to consider

There are a number of regulations and standards that organisations must comply with in order to effectively implement a security governance framework. Owners and operators of critical infrastructure must understand that managerial and organisational liability for information security continues when IT functions are outsourced. In addition, if the outsourcing is not properly managed and associated risks understood, the blurring of organisational boundaries and responsibilities can in fact increase information security risks.

Organisations can be liable for negligence, breach of contract and liability for breaches of legislation such as the *Corporations Act 2001*, the *Trade Practices Act 1974* and the *Cybercrime Act 2001*. Further, the *Privacy Act 1998* imposes obligations on the way organisations collect, retain, use and disclose personal information. A summary of some of the more common regulatory compliance requirements for Australian organisations is set out at Attachment A.

There are strong legislative and prudential standards relating to IT security, data protection and risk management operating in Australia. There may also be obligations imposed by industry-specific legislation. For example, the Australian Prudential Regulation Authority (APRA) has released new standards concerning outsourcing by Authorised Deposit-taking Institutions, or 'regulated' institutions such as banks, building societies, and credit unions<sup>8</sup>. You should be aware of any legislation applicable to your industry and seek professional advice if you are unsure of your organisation's obligations.

Two international standards can assist organisations with outsourcing: *ISO 27001 Certification* is highly desirable for helping companies comply with legislation and instilling consumer confidence, and organisations can use the standard *AS/ISO 17799: 2006 Code of practice for information security management* as a basis to identify the control areas to be specified in the outsourcing agreement.

## **2.2 Effectively managing security in the outsourcing process**

An organisation needs to consider its in-house capability to effectively manage IT security in an outsourcing arrangement. If an organisation is not confident of its capability in this area, it should consider contracting this function to a qualified third party. This is important as an organisation has a responsibility to ensure that effective security processes are implemented and checked, not only with the IT service provider, but also with any subcontractors used by the service provider.

Accordingly, prior to entering into an outsourcing arrangement, an appropriate organisational IT security strategy should be put in place and uniformly incorporated into each outsourcing contract to ensure consistency. This will:

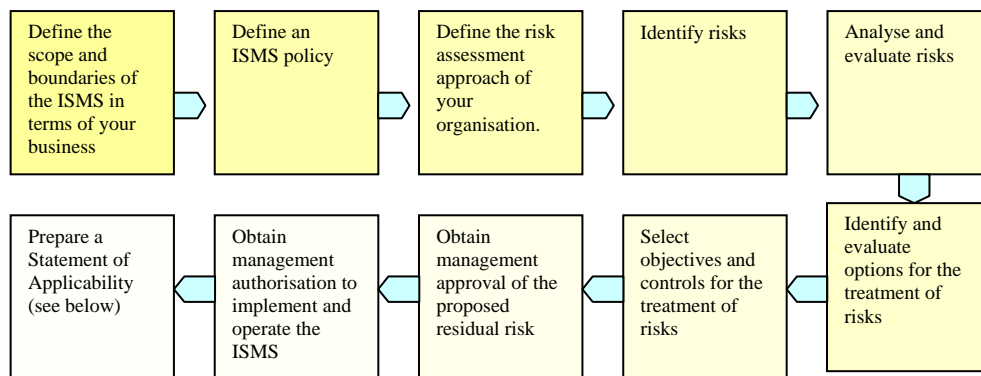
- enhance consistency between outsourcing contracts and the organisation-wide strategy;
- make administration more efficient;
- increase the likelihood of overall compliance; and
- allow for easier detection of systemic and organisational issues.

*AS/NZS ISO/IEC 27001* is a Standards Australia standard used to specify the requirements for an effective Information Security Management System (ISMS) model. According to *AS/ISO 27001:2006*, an ISMS should follow a model illustrated in Figure 6.

---

<sup>8</sup> 'APRA Prudential Practice Guide, PPG 231- Outsourcing, March 2006', [www.apra.gov.au](http://www.apra.gov.au).

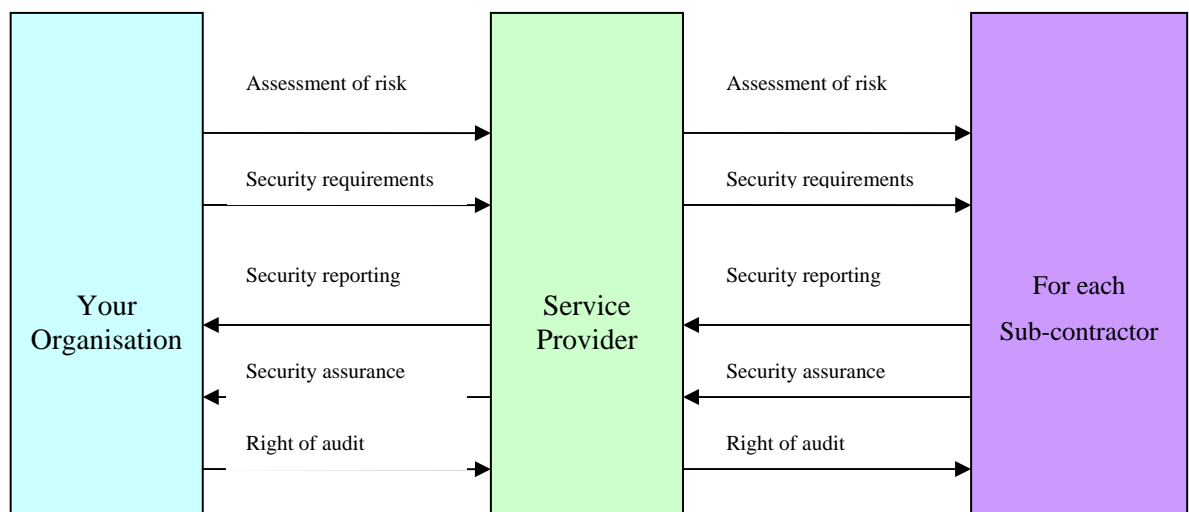
Figure 6—ISMS model



Note 1: A Statement of applicability shows the controls that have been selected, or not selected from *ISO 27001* and the reason for their selection, or non-selection. It must also show the controls currently implemented.

The information security management process illustrated in Figure 7 shows the development of the relationship between your organisation and the service provider and shows how the flow of information concerning risk assessment, security requirements, reporting, security assurance, and right of audit should be managed.

Figure 7—Flow of risk management information in an outsourcing arrangement



In the case of an outsourcing arrangement, if your service provider subcontracts work related to your IT functions, they should repeat the outsourcing information security management process with each subcontractor, such that the ISMS covers the entirety of the information and systems outsourced by the organisation. This should be dealt with in the initial outsourcing contract.








### 2.3. Risk assessments

Due to the central role of ICT in most outsourcing arrangements, IT security risk becomes relational to other business risks, such as intellectual property and customer data. If your organisation is entering into an IT outsourcing arrangement, the organisation has a responsibility to ensure that the risk and compliance requirements of the outsourcing arrangements are clearly understood by the IT service provider.

Your organisation can be expected to articulate the IT security requirements clearly, ensure that risks are properly managed, and that reporting and corrective systems are in place. Strategies should be implemented so that identified risks are treated to the degree that they become acceptable risks. This should flow down the line if your service provider is going to use subcontractors to perform some of the outsourced IT functions.

An assessment of security risks should be undertaken prior to a decision to enter into an outsourcing arrangement. Some general steps in undertaking a risk assessment are detailed in the check list below:

*Figure 8—Risk assessment check list*

<p><b>Identify</b> the business processes and functions whose underlying information systems are to be outsourced, based on the scope of the intended outsourcing.</p>	 
<p><b>Identify</b> for each business process or system, the specific governance, regulatory or compliance standards, key technical strategies or architectures, or other material constraints which apply to your organisation and its industry sector, and the implications of those constraints.</p>	
<p><b>For each</b> business process or system, carry out a Business Impact Assessment to understand the impact of loss of confidentiality, integrity or availability of the system, using a scale of impact levels for each of confidentiality, integrity and availability.</p>	
<p><b>Assess</b> the security threats to your organisation and its systems, either accidental or malicious, in terms of the people/organisations that might attack it, and their motivation and capability to do so.</p>	
<p><b>Review</b> the current vulnerabilities and compliance status of each system, particularly against national and international standards.</p>	
<p><b>Identify</b> the gap between the current level of residual risk and compliance and the target level of residual risk and compliance when outsourced.</p>	

Note 2: See also the Standards Australia publication, 'HB 231–2004—Information Security Risk Management Guidelines'.

## **2.4. Transitional arrangements**

In order to enable your chosen IT service provider to step into its role with a minimum of inconvenience and potential problems, your outsourcing contract should also deal with issues arising during this transition phase (and also during any transition occurring upon termination or expiration of the contract).

To ensure IT security risks continue to be managed during the transition period, your organisation and the IT service provider should jointly develop a security management transition plan, which should in turn form part of the contract. The plan should have three phases:

- the transition of current security operations to the service provider—a joint responsibility;
- the implementation of the Information Security Management System which meets the risk assessment, compliance requirements, control specification and other contractual requirements—this is the service provider’s responsibility; and
- a post-implementation assurance review in a form specified by your organisation, compatible with the security management approach used<sup>9</sup>.

## **2.5. Issues to be addressed in the contract**

In addition to the issues and risks identified above, there are a number of additional, specific matters which need to be considered and addressed, either in the outsourcing contract or, where appropriate, in separate documents.

As set out above, the broad stages which require consideration in ensuring information security in outsourcing arrangements are as follows:

1. Ensure appropriate internal information security management system (ISMS) in place;
2. Identification, assessment and evaluation of risks;
3. Procurement security steps;
4. Roles and responsibilities;
5. Contracting for information security;
6. Transitional security arrangements;
7. Assurance and conformance;
8. Ongoing security management (including change management);
9. Incident management and reporting; and
10. Termination and transition.

Attachment C sets out these steps, together with some of the tasks which may need to be performed at each stage and external reference material which may be of assistance.

Some examples of particular issues for consideration follow:

---

<sup>9</sup> *Good Practice Guide—Outsourcing: Security Governance Framework for IT Managed Service Provision*, 2 August 2006, UK National Infrastructure Security Co-Ordination Centre), p 22

### **2.5.1. Protecting customer and client information**

Where an IT service provider or potential provider is likely to have access to confidential customer data, business information, or other protected information in the course of a procurement process, it is necessary to take some basic steps to ensure that the information does not leak. They can include:

- ensuring appropriate and effective confidentiality agreements are in place; and
- taking steps within the procurement framework to review the internal security measures and policies of service providers.

### **2.5.2. Incident management**

Your organisation should contractually oblige the IT service provider to report to a nominated contact within your organisation on an agreed timely basis and format all security related:

- incidents (such as a detected abnormality in an operating environment);
- suspected or suspicious incidents;
- successful or unsuccessful compromises;
- anomalies;
- contact by law enforcement, regulatory or security authorities; and
- civil injunctions or search orders.

You should agree with the service provider in the contract how security incidents should be investigated and corrective actions taken—particularly those to be taken in an emergency. You should also ensure that the contract reflects your organisation's requirements for the handling of confidential customer data, business information, or other protected information by imposing requirements on the service provider such as that they must not disclose this type of information, and that in instances where the service provider may be required to do so by law they must let your organisation know.

In addition to conventional contingency planning and disaster recovery, you should agree with the service provider about managing incidents involving sustained electronic attacks which may threaten the ability of the service provider to continue to operate the service in accordance with the security control requirements.

### **2.5.3. Monitoring and reporting requirements**

A key part of managing security in outsourcing arrangements is gaining assurance that risks have been managed, are being managed, and will continue to be managed. Outsourced systems often involve such corporate risk in terms of overall business continuity, loss of reputation and/or regulatory non-compliance that organisations cannot wait for an incident to happen and then seek to claim damages.

Attachment B sets out some of the existing methods of assurance which are currently available to organisations in outsourcing arrangements.

Under *AS/ISO27001* certification, a service provider is obliged to commission an independent accredited certification firm to review the ISMS against *ISO27001* and issue a certificate.

The Information Systems Audit and Control Association's (ISACA) COBIT<sup>10</sup> provides a framework from which overall IT governance maturity can be assessed<sup>11</sup>.

COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximising the benefits derived through the use of information technology and developing appropriate IT governance and control in a company.

The service provider should be obliged contractually to provide regular reports on performance of the outsourced functions, with specific reference to information security:

- (a) incidents;
- (b) emerging threats; and
- (c) changes to the regulatory environment affecting both the organisation and the service provider.

#### **2.5.4. Making the contract responsive to change**

Most large contracts need to change over their course. These changes may relate to security, either because changes in the scope, functionality or performance of systems impact on security, or because the security requirement itself has changed.

#### **2.5.5. A change in management**

Contractual change management boards should have representation by qualified and experienced security professionals from both your organisation and the service provider.

As changes often lead to additional costs, the contract should clearly address, for security-related changes, which changes should be paid for by your organisation as a 'scope change', and which changes should be absorbed by the service provider.

#### **2.5.6. Changes in risk, security needs and compliance**

Performance of security against requirements should form a key part of the contract's service level agreements which are monitored and linked to contractual bonuses or performance penalties.

Processes should be put in place contractually for ongoing management of the security relationship with the service provider, covering:

---

<sup>10</sup>

[www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981](http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981)

<sup>11</sup> The relationship between COBIT, ITIL and ISO27001 is usefully described in 'Aligning COBIT, ITIL and ISO 17799 for Business Benefit' at [www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22490%20](http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=22490%20)

- changes in risk (including business processes, business impact, threat and vulnerability);
- changes in regulatory or compliance requirements;
- changes in security requirements, including control specifications,
- commissioning of, results of, and corrective actions from security performance and assurance reporting; and
- access control changes relating to security.

A procedure should be contractually agreed to between your organisation and the service provider for any new system or changes to systems which may have a material effect on IT security.

### **2.5.7. Termination and transition arrangements**

A contract can be ended (discharged) for a number of reasons: because all obligations have been fulfilled; due to mutual agreement; or due to underperformance, a breach of contract, or as a matter of convenience<sup>12</sup>. Risks at this stage of the contract lifecycle can include:

- the service provider's failure to return all required materials; and
- disagreement with regard to a final payment, or the submission of unforeseen additional costs by the service provider;

There are additional risks to consider if you are discharging an agreement with one service provider and transitioning your IT functions to another service provider.

These include:

- failure to properly manage the transition process;
- disruption to the provision of products and services; and
- failure to address performance problems (particularly if the impetus for termination and transition was poor performance) within the previous outsourcing arrangements.

Note 3: If you have discharged a contractual arrangement, and begin a tender process to engage another service provider, you should manage the process of re-tendering in line with probity requirements, particularly where the existing (or previous) service provider is re-tendering. The existing, or previous service provider, must be treated in the same way as any other tender applicant. You should also ensure that the existing, or previous service provider is only privy to information about the process that is freely available to other tender applicants.

Your organisation's contract with the IT service provider should cover how security will be managed in event of termination and/or the transition of the contract. It should clearly define the following:

- Upon transition:

---

<sup>12</sup> *Developing and Managing Contracts, Getting the Right Outcome, Paying the Right Price*, ANAO Best Practice Guide, February 2007, p 100  
[www.anao.gov.au/](http://www.anao.gov.au/)

- how the service provider works with the new service provider to transition outsourced IT systems in accordance with an agreed service termination process;
- what arrangements are in place to ensure that the ISMS is transitioned to the new IT service provider in accordance with a contractually agreed ISMS termination plan;
- assurance that a transition will be properly managed and that there will be minimal disruption to services;
- that an evaluation will be conducted in relation to the performance of the contract, service provider and your organisation, and that any 'lessons learned' will be incorporated into new arrangements, and if necessary, requirements to update internal policies and procedures to reflect any lessons learned.
- Upon termination:
  - that the service provider will supply your organisation with documents, files, procedures, configurations, drawings or records relating to your organisation's services, and destroy all information on storage media such as disks and tapes;
  - record and make clear any intellectual property rights;
  - ensure that there are sufficient steps taken to terminate access rights or arrangements, which can include making sure that all administrative accounts are disabled or reset, and that all remote management systems are disabled or blocked; and
  - that deliverables are supplied in accordance with agreed standards and that triggers for final payment are articulated.

### **3. Resources**

#### **Standards Australia**

*HB 280–2006, Case Studies—How Boards and Senior Management Have Governed ICT Projects to Succeed (or Fail)*, Standards Australia, Sydney, 2006

*AS/NZS ISO/IEC 27001:2006, Information technology—Security techniques—Information security management systems—Requirements*, Standards Australia, Sydney, 2006

*AS 8015–2005, Corporate Governance of Information and Communication Technology*, Standards Australia, Sydney, 2005

*HB 240–2004, Guidelines for Managing Risk in Outsourcing Utilizing the AS/NZS 4360:2004 process*, Standards Australia, Sydney, 2004

*AS/NZS ISO/IEC 17799:2006, Information technology—Security techniques—Code of practice for information security management*, Standards Australia, Sydney, 2006

Bezzina, Mark. *Security Standards and Support Systems Report*, Standards Australia, Sydney, 2006

#### **Trusted Information Sharing Network**

*Leading Practices and Guidelines for Enterprise Security Governance*, June 2006

*IT Security Governance for Board of Directors and CEOs*, June 2006

*CIO, CISO and Practitioner Guide: IT Security Governance*, June 2006, sourced from: [www.tisn.gov.au](http://www.tisn.gov.au).

#### **Australian Prudential Regulation Authority**

APRA Prudential Practice Guide, *PPG 231—Outsourcing, March 2006*, [www.apra.gov.au/Policy/Prudential-Standards-Guidance-Notes-for-ADIs.cfm](http://www.apra.gov.au/Policy/Prudential-Standards-Guidance-Notes-for-ADIs.cfm)

#### **Other Articles**

Rottman, Joseph W and Mary C Lacity, 'Proven Practices for Effectively Offshoring IT Work', MIT Sloan Management Review, Vol. 47, No. 3, pp. 56–63, 2006

Overby, Stephanie, 'Just Say "Know": It's a scenario scary enough', CIO, November, p. 41, 2006

*Outsourcing: Security Governance Framework for IT Managed Service Provision*, Centre for the Protection of National Infrastructure, August 2006  
[www.cpni.gov.uk/Products/guidelines.aspx](http://www.cpni.gov.uk/Products/guidelines.aspx)

# Attachment A

## ***Regulatory and Risk Environment***

### **Compliance with legal requirements**

Most guidelines and standards dealing with information security refer to the need for legal compliance. Organisations, their directors, senior managers and staff can incur civil and/or criminal liability under the general law and statutes even though they had not participated directly in a wrongful act. Examples include:

#### **Cybercrime Act**

The *Cybercrime Act 2001 (Cth)*, which commenced on 2 April 2002, introduced a new part to the *Criminal Code Act 1995 (Cth)*. The new part contains new computer offences designed to address forms of cybercrime which impair the security, integrity and reliability of computer data and electronic communications.

#### **Corporate culture offences**

The *Commonwealth Criminal Code* also provides that companies can be liable for certain offences committed by employees where the company has a 'corporate culture' which tolerates breach of Commonwealth laws (Section 12). These provisions go against the commonly held view that a person can only be criminally liable if they have a guilty mind (Section 12.3).

The term 'corporate culture' is defined as an attitude, policy, rule, course of conduct or practice existing in the company. The effect is that if management have created a culture of non-compliance with Commonwealth laws, then the company can also be prosecuted for committing the offence.

#### **Trade Practices Act (TPA) liability**

Under Section 52, TPA liability can arise for a corporation, its directors and high level managers where the corporation represents (typically in its Privacy Policy or contractual undertakings) that the information that customers or suppliers provide to the corporation is 'secure'. Should there be a disclosure or corruption of information held by the corporation without adequate protective measures being in place, there is potential for such a representation to be found to be misleading and/or deceptive, and not only the corporation, but also its directors and senior managers can be found to be in breach of the TPA and personally liable for damages suffered as a consequence.

#### **Contractual breach**

Contractual arrangements between a customer and a provider typically contain clauses protecting their respective confidential information and undertakings as to system security.

Breaches of such clauses may entitle the injured party to common law remedies. Remedies may include claims for specific performance or termination of the contract and/or damages.

Given the increasing monetary and strategic value of confidential information and systems, claims for damages can be substantial.

## **Torts and claims for negligence**

The purpose of the law of torts is to recompense wronged and injured parties for losses and afford compensation for loss or injury sustained as the result of the negligent activities of others.

A Denial of Service (DOS) attack is a typical example where the law of tort and negligence may provide a remedy. DOS attacks are unique in that the perpetrators use other people's computers to launch the attacks and the hijacked sites are both victims and culprits. (See *Denial of Service/Distributed Denial of Service Report*; *Denial of Service/Distributed Denial of Service: Advice for CEOs*; *Denial of Service/Distributed Denial of Service: Advice for CIOs* at: [www.tisn.gov.au](http://www.tisn.gov.au).)

The appropriate standard of care is judged by balancing the seriousness of the harm likely to ensue, the likelihood of the harm eventuating and the expense, difficulty and inconvenience involved in taking preventative measures.

If corporations, their directors and staff fail to exercise proper judgement or fail to take adequate steps to protect against loss or damage suffered from DOS attacks, they may face significant claims.

### **Vicarious liability**

An organisation, as employer, may be vicariously liable to third parties for tortious acts of their employees which are impliedly authorised, that is, acts committed while the employee is acting within the scope of the employee's authority and performing the employment duties or acts incidental to the performance of such duties.

Employees may cause a breach of information security in respect of information stored in an organisation's systems by causing a firewall to be disengaged, intentionally disclosing client information or opening work related or non-work related emails containing viruses.

By providing powerful computing facilities to employees, the employer increases the ways in which its employees can commit civil and criminal offences, exposing the employer to new forms of liability. Unless the employer takes appropriate steps to educate, monitor and control the employee's access and use of such technology, the employer may incur liability.

### **Privacy Act liability**

The *Privacy Act 1988* enjoys broad application, and impacts on Information Security. Other than specified exceptions, organisations with an annual turnover of more than \$3 million are bound by the private sector provisions of the *Privacy Act*, including the National Privacy Principles. Under National Privacy Principle 4 (NPP 4), organisations have an obligation to secure all personal and sensitive information that is contained or passes through their systems. NPP 4 requires organisations to take all reasonable steps to:

- (a) protect personal information it holds from loss, misuse, unauthorised access, modification and disclosure; and
- (b) destroy or permanently de-identify personal information it no longer needed for the purpose it was disclosed.

An offending organisation's risk following proven non-compliance includes legislative penalties and lawsuits for damages as well to reputation and brand damage.

Guidelines to the National Privacy Principles can be obtained from the Office of the Privacy Commissioner's website, at [www.privacy.gov.au](http://www.privacy.gov.au).

### **General law liability of Directors**

The law as established by Australian courts imposes the following duties on directors and officers of corporations:

- (a) to act in good faith in the best interest of the corporation; and
- (b) to exercise their powers for a proper purpose with care and diligence.

The courts, in applying these duties, consider what a reasonably prudent and knowledgeable person, knowing the internal and external information security threats to the corporation and its business would have done to prevent damage or loss. A court can find that directors or officers breached one or more of their duties by failing to take action or adequate steps to prevent damage or loss in which case directors and officers can be held personally liable.

### **Corporations Act duties**

Section 180 of the *Corporations Act 2001 (Cth)* incorporates and extends some of the general law principles. The section requires in addition that directors and officers make informed decisions and make decisions which they believe to be in the best interest of the company.

The Section applies a business judgment rule meaning that directors and officers need to take all relevant facts into consideration, including advice received from employees and/or professionals and make a decision in the best interest of the company. If directors or officers knew or have been advised of information security risks and fail to take adequate steps to protect the company against those risks, they may be personally liable for their failure.

### **Obligations under foreign laws**

Where an organisation is trading with foreign companies, has a foreign parent company or has financial, commercial, retail, distribution or other links to other jurisdictions, it is important to be aware that the laws of the foreign jurisdiction may apply to and bind your organisation. You should obtain independent legal advice if you are unsure as to your obligations under the laws in another jurisdiction with which your organisation has a nexus when negotiating and finalising an outsourcing contract.

## Attachment B

### ***Security Requirements, Communication, Management and Assurance Approaches***

The table below summarises security requirements that should be communicated, and management and assurance approaches which are likely to help ensure that risks are managed in accordance with your organisation’s expectations.

<i>Security requirement</i>	<i>Approach</i>	<i>Features</i>
1. Detailed controls specification	<p>Organisation specifies in detail:</p> <ul style="list-style-type: none"> <li>• the assessment of risk;</li> <li>• the compliance requirements;</li> <li>• the security requirements in terms of the detailed controls to be employed; and</li> <li>• the level to which those controls are employed for every system in the inventory of the services being outsourced.</li> </ul> <p><i>AS/ ISO 17799:2006</i> may be used as a basis to identify the control areas to be specified, though other security standards may be used.</p> <p>A detailed system-specific security policy is contractually invoked for each system (or group of systems).</p> <p>Provider operates security in accordance with the detailed system—specific security policy, developing whatever</p>	<p>The organisation is likely to spend considerable security professional resources specifying and negotiating the controls with the provider.</p> <p>The organisation can be specific about its security requirements and controls.</p> <p>The provider is likely to be constrained in what they can and cannot do.</p> <p>The organisation takes responsibility for the fitness for purpose of the detailed controls specification.</p> <p>Any control not specified will not be carried out by the provider—the control specification is likely to override any intent implied in communication of risk assessments or compliance requirements.</p>

	<p>technical configurations, standards, procedures, records or processes are required to implement the controls. The organisation should specify as part of the system-specific security policy which elements of the controls are to be documented and supported by retained, documented records.</p> <p>Organisation gains assurance from a combination of:</p> <ul style="list-style-type: none"><li>• security performance reporting; organisation-commissioned security audits;</li><li>• reports from provider-commissioned security audits; and</li><li>• letters of representation from provider.</li></ul> <p>Organisation requires provider to use a similar approach with all subcontracts (and sub-subcontracts).</p>	
--	---	--

<i>Security requirement</i>	<i>Approach</i>	<i>Features</i>
<p>2. Control objective based specification with independent third party review (COBIT)</p>	<p>The organisation specifies in detail:</p> <ul style="list-style-type: none"> <li>• the assessment of risk;</li> <li>• the compliance requirements; and</li> <li>• invokes them within the contract.</li> </ul> <p>The customer develops a set of high- level control objectives in conjunction with the provider and a third party independent auditor.</p> <p>Provider transforms high-level objectives into detailed system security policies, procedures, physical security, technical configurations and personnel security measures (perhaps using <i>ISO17799:2006</i> as a guide for completeness).</p> <p>Provider operates system in accordance with detailed system security policies.</p> <p>The organisation contractually requires provider to provide a management attestation and to commission a third party audit review, for example using SAS70 principles and which may be a formal SAS70 audit, to provide assurance that control objectives have been complied with.</p> <p>The organisation requires provider to use a similar approach with all subcontracts (and sub-sub contracts).</p>	<p>The organisation is likely to spend less professional security resources on detailed controls specification.</p> <p>Provider has considerable flexibility in determining how to meet the requirements of the control objectives.</p> <p>Provider costs may increase due to the need to commission third party audit work.</p> <p>Assurance approach inherently integrated with the security management approach and can meet assurance requirements of regulatory compliance reporting.</p> <p>Third party review opinion by regulated audit firm can provide strong reliance due to the liability taken on by the auditor.</p>

<i>Security requirement</i>	<i>Approach</i>	<i>Features</i>
<p>3. AS/ ISO 27001 ISMS with certification</p>	<p>The organisation and provider agree the risk assessment, compliance requirements specification and control objectives to be used as the basis of the <i>ISO27001 ISMS</i>.</p> <p>The <i>AS/ISO27001</i> Statement of Applicability is defined to include the entire scope of the outsourcing contract and all people, processes, facilities and systems supporting it if full coverage is to be achieved.</p> <p>Provider implements, operates, monitors, reviews, maintains and improves the ISMS in accordance with <i>ISO 27001</i>, carrying out all <i>ISO27001</i> requirements.</p> <p>Provider commissions <i>ISO27001</i> registered auditor to review the ISMS and grant <i>ISO27001</i> certification.</p> <p>At the organisation's option, the provider contracts with a regulated audit firm who are also registered <i>ISO27001</i> auditors to provide dual assurance, comprising <i>ISO27001</i> certification and a <i>SAS70</i> opinion. The organisation requires provider to use a similar approach with all subcontracts (and sub-sub contracts).</p>	<p><i>ISO27001 ISMS</i> involve considerable formalised processes and documentation. This is likely to be costly to implement on a custom IT outsourcing operation, but may be cost-effective when using components of leveraged, shared infrastructure. It is vital to ensure that the risk assessment, control objectives and Statement of Applicability represent the organisations' risk assessment, control requirements and contract scope for a certification to be relied upon.</p> <p><i>ISO27001</i> audits are often procedural in nature, with the certification company accepting little legal liability to those to whom the certificate is granted, and none to those relying on it.</p>

## Attachment C

### Key Elements and Tasks—Outsourcing and Information Security

<i>Step</i>	<i>Description of Element</i>	<i>Tasks</i>	<i>External Reference Material</i>
1.	Ensure appropriate internal information security management system (ISMS) in place	<ul style="list-style-type: none"> <li>- Draft ISMS</li> <li>- Implement ISMS, including appropriate training for staff</li> <li>- Maintain and periodically review ISMS</li> </ul>	<ul style="list-style-type: none"> <li>- AS 27001:2006</li> <li>- AS 8015:2005</li> </ul>
2.	Risk Management—Identification, assessment and evaluation of risks	<ul style="list-style-type: none"> <li>- Identify risks relevant to proposed outsourced task</li> <li>- Analyse and evaluate risks in accordance with HB 231:2004</li> <li>- Take steps to treat risks where appropriate</li> <li>- Where risks are to be accepted, ongoing monitoring and review of risks</li> </ul>	<ul style="list-style-type: none"> <li>- HB 231:2004</li> <li>- AS/NZS 4360:2004</li> </ul>
3.	Procurement security steps	<ul style="list-style-type: none"> <li>- Confidentiality agreements to be executed by potential tenderers, if appropriate</li> <li>- Steps to be taken (within the procurement framework) to review the internal security measures and policies of tenderers</li> </ul>	<ul style="list-style-type: none"> <li>- AS 17799:2006</li> </ul>
4.	Defining roles and responsibilities	<ul style="list-style-type: none"> <li>- Upon selection of a successful tenderer, roles and responsibilities to be outlined to ensure: <ul style="list-style-type: none"> <li>- awareness of security risks by both parties;</li> <li>- agreement as to which party is managing which risks;</li> <li>- accountability for security risk management;</li> <li>- consistency of security policies and levels;</li> <li>- no duplication of effort or confusion as to accountability; and</li> <li>- sufficiency of security measures across the board</li> </ul> </li> </ul>	

<i>Step</i>	<i>Description of Element</i>	<i>Tasks</i>	<i>External Reference Material</i>
5.	Contracting for information security	<ul style="list-style-type: none"> <li>- Agreement between the parties should reflect the following: <ul style="list-style-type: none"> <li>- risks which have been identified at step 2 of the process;</li> <li>- risks which may arise during the course of the contract—it is important to ensure that the contract captures these in broad terms; and</li> <li>- responsibilities for day-to-day security management requirements</li> </ul> </li> </ul>	
6.	Transitional security arrangements	<ul style="list-style-type: none"> <li>- A security management transition plan should be developed to transition current security operations to the provider, and transition the ISMS into one which meets the requirements set out in the agreement between the parties.</li> </ul>	<ul style="list-style-type: none"> <li>- AS 27001:2006</li> <li>- AS 8015:2005</li> </ul>
7.	Assurance, reporting and conformance	<ul style="list-style-type: none"> <li>- The contract should provide for review and audit mechanisms, to ensure ongoing compliance with the security requirements.</li> <li>- Options available for audit or certification include: <ul style="list-style-type: none"> <li>- SAS70 Review—provider is required under the contract to commission a review by an independent regulated auditor; and</li> <li>- AS/ISO27001 Certification—provider commissions an independent accredited certification firm to review the ISMS against AS27001 and issue a certificate.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- SAS70</li> <li>- AS/ISO27001:2006</li> <li>- COBIT</li> </ul>
8.	Ongoing security management (including change management)	<ul style="list-style-type: none"> <li>- Operational review of the security arrangements and standards should be provided for in the contract and performed from time to time.</li> <li>- The contract should also include regular reporting obligations (independent of incident reporting).</li> <li>- Where change to the contract is likely to arise for security reasons, the contract should deal with responsibility for any additional costs.</li> </ul>	

<i>Step</i>	<i>Description of Element</i>	<i>Tasks</i>	<i>External Reference Material</i>
9.	Incident management	<ul style="list-style-type: none"> <li>- The provider should be required to report to the organisation in relation to any incidents, suspected incidents, successful compromises, unsuccessful compromises, anomalies, contact by law enforcement or other authorities or civil injunctions or search orders.</li> <li>- A plan must be in place for disaster recovery, management of security incidents and any incident involving a sustained electronic attack.</li> </ul>	
10.	Termination and transition	<ul style="list-style-type: none"> <li>- The contract must cover the steps to be taken upon termination of the contract, including in particular: <ul style="list-style-type: none"> <li>- transition of the systems in such a way as to maintain security of data and systems; and</li> <li>- return and/or destruction of any confidential or protected materials.</li> </ul> </li> </ul>	