TISN

FOR CRITICAL INFRASTRUCTURE

RESILIENCE

Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers)

Executive Overview Supplement

June 2011

DISCLAIMER: This document is intended as a general guide only. To the extent permitted by law, the Australian Government makes no representations or warranties of any kind, express or implied, about the accuracy or completeness of the material contained in the document. The reliability of any assessment or evaluation based on its content are matters for the independent judgement of users. Users should seek professional advice as to their specific risks and needs. The Australian Government accepts no responsibility for the consequences of any use of this document.

This Page is Intentionally Blank

.

Foreword

This Executive Overview is a supplement to the *Securing Information in an Outsourcing Environment (Guidance for Critical Infrastructure Providers)* guide. The supplement is intended to provide senior executives from Australian critical infrastructure providers with a useful high-level guide, which may assist with the consideration of potential information security issues prior to the establishment of outsourcing arrangements.

The full guide also examines the potential information security issues and nuances related to the use of "cloud computing" for the delivery of outsourced services. For the purposes of this supplement, the principles and guidance covered apply equally to an outsourced arrangement that utilises both traditional and "cloud-computing" delivery mechanisms.

The Department of Broadband, Communications and the Digital Economy (DBCDE) on behalf of the IT Security Expert Advisory Group (ITSEAG) of the Trusted Information Sharing Network (TISN) has prepared this supplement.

This supplement and associated guide builds upon the previous guide, published by DBCDE in 2007, relevant standards and guidance as well as referencing information contained within the Centre for the Protection of National Infrastructure's (UK) document entitled, *'Outsourcing: Security Governance Framework for IT Managed Service Provision (Version 2, 2009)'*[1].

DBCDE would like to thank the UK Government for allowing the Australian Government to reference their published guidance on this resource. DBCDE would also like to acknowledge the active involvement of the ITSEAG members throughout the preparation of the Guide.

The associated guide, which provides further detail on securing information in an outsourcing environment, is available on the TISN website for download.[2].

ITSEAG Secretariat
Communications Critical Infrastructure Resilience
Department of Broadband, Communications and the Digital Economy
Email: itseag@dbcde.gov.au
Web: www.dbcde.gov.au and www.tisn.gov.au

[1] Available at *www.cpni.gov.uk/Products/guidelines.aspx*
[2] Available at *www.tisn.gov.au*

1. Why is it important to maintain sound information security in an outsourcing arrangement?

Outsourcing of IT services can provide an organisation the opportunity to realise valuable strategic and economic benefits. However, for senior executives in organisations responsible for the delivery of critical infrastructure services, the careful consideration of risks and threats, the structure of contractual arrangements and compliance obligations is of paramount importance prior to the commencement of any outsourcing arrangement.

> ***Risk comes from not knowing what you are doing.***
>
> *Warren Buffet*

Senior executives in critical infrastructure organisations have the responsibility to ensure that their organisation designs and implements sound information security principles and practices throughout each and every business process.

Should the organisation under fail to adequately consider the range of information security risks and threats that could compromise the integrity, availability and performance of the organisation's services delivered through an outsourcing arrangement, the resultant impacts, both personally and corporately, may include:

- lack of compliance to legislative obligations, resulting in exposures to potential litigation;
- the inability to provide critical services to the community leading to potential national security exposures; and
- the implantation of costly remediation activities to rectify the service provision in the event of an information security incident.

Further to these potential exposures, it is important for senior executives within critical infrastructure organisations to understand that whilst the establishment of an outsourcing arrangement may transfer the delivery of a business function to a third party - the ultimate responsibility for the design and implementation of information security policies, regulatory compliance, and control execution still resides with the senior leadership of the organisation.

> ***Services may be outsourced but risks and regulatory compliance remain the responsibility of the Critical Service organisation.***

This supplement raises at a high level, information security issues that should be considered by senior executives, the establishment of sound information security foundations inside an organisation and a brief discussion on where to from here when considering the establishment of an outsourcing arrangement. This supplement is intended to provoke dialogue between senior executives and their staff on the potential risks in an outsourcing arrangement.

2. Information Security in an Outsourcing Environment; Senior Executive Considerations

Is outsourcing suitable for an organisation's service delivery?

The organisational drivers for establishing an outsourcing arrangement may include cost savings, increased business flexibility, exploitation of new technologies and accessing specialist expertise as well as government directives.

> Outsourcing as a sourcing option, refers to an arrangement by which a task (s) that would otherwise be performed by staff internal to the organisation is transferred to an external entity specialising in the management and delivery of the task (s).

As a result, outsourcing involves transferring or sharing management control of a business function, enabled by two-way information exchange, coordination, and trust between the outsourcer and the client.[3]

It is important to understand that responsibilities and controls must remain in place for services, whether internally managed or outsourced, including with any third party providers, and particularly in regards to information security.

As with all outsourcing arrangements, senior executives should carefully consider the nature of the information being handled by the third party provider prior to the organisation assessing the potential benefits of an outsourcing arrangement. If the information under management is deemed to be classified or sensitive in its nature, a senior executive should ensure that the assurance over the integrity and security of the information can be adequately protected. If such assurance cannot be maintained effectively within an outsourcing environment, a senior executive should have the organisation explore alternative delivery mechanisms.

What is Information Security? And why is it essential in an outsourcing environment?

Information security is the protection of information and information systems and encompasses all infrastructure that includes processes, systems, services, and technology. It relates to the security of any information that is stored, processed or transmitted in electronic or similar form.

Information security has the following objectives:

Confidentiality – Ensuring that information is accessible only to those with a legitimate requirement and authorised for such access;

Integrity - Safeguarding the accuracy and completeness of information and processing methods; and

Availability - Ensuring that authorised users have access to information and associated assets when required.[4]

[3] *Secure Your Information – Information Security Principles for Enterprise Architecture: Report,* TISN, Sept 2007, p 52 http://tisn.gov.au/www/tisn/content.nsf/Page/Publications

[4] *Protective Security Policy Framework,* Australian Government Attorney-General's Department, Jan 2011, p 24

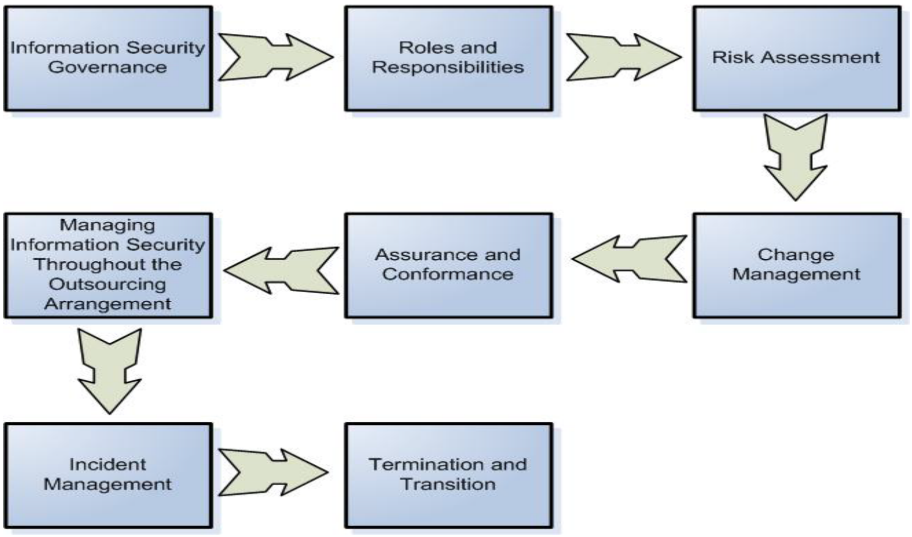
Underpinning these objectives are a set of information security principles outlined by the ITSEAG paper *Secure your Information: Information Security Principles for Enterprise Architecture*[5], as follows:

1. Information Security is Integral to Enterprise Security;
2. Information Security Impacts on the Entire Organisation;
3. Enterprise Risk Management defines Information Security Requirements;
4. Information Security Accountabilities should be Defined ad Acknowledged;
5. Information Security must consider Internal and External Stakeholders;
6. Information Security requires Understanding and Commitment; and
7. Information Security requires Continual Improvement.

As a senior executive responsible for the provision of critical infrastructure services, it is essential that the organisation has ensured that these information security principles have been assessed prior to embarking on an outsourcing arrangement and that appropriate auditing and assurance mechanisms can be effectively implemented.

3. Establishing Sound Information Security Foundations in an Outsourcing Arrangement.

As discussed previously, in any outsourcing arrangement the responsibilities of senior executives includes ensuring that sound information security foundations have been established and can be maintained throughout the arrangement. The figure below shows the eight information security management elements that should be established by an organisation in an outsourcing arrangement. In order to promote a truly effective information security management approach, each of these elements requires the same priority and focus from both senior executives and the wider organisation.


Information Security Governance
Roles and Responsibilities
Risk Assessment
Change Management
Assurance and Conformance
Managing Information Security Throughout the Outsourcing Arrangement
Incident Management
Termination and Transition

[5] *Secure your Information: Information Security Principles for Enterprise Architecture*, Department of Broadband, Communications and the Digital Economy, Information Technology Security Expert Advisory Group, June 2007, Executive Summary

Information Security Governance

It is important for senior executives to understand their role in planning, implementing and maintaining effective information security governance in organisations. Information security governance defines the security principles, accountabilities, and actions required by an organisation to achieve their identified security objectives.

Information security governance should align to all other governing areas within an organisation, forming part of the overall corporate governance of an organisation and should be comprised of staff with the appropriate skills and experience to advise the senior executives of potential issues requiring attention and/or remediation.

In an outsourcing arrangement, information security must be comprehensively addressed at all stages, including prior to the arrangement being established, throughout the operation of the arrangement and during termination or transition.

Roles and Responsibilities

In any outsourcing arrangement, the establishment of clear roles and responsibilities between an organisation's management and the outsourcing provider is essential. Underpinning the establishment of clear roles and responsibilities is the drafting and execution of clearly articulated contractual arrangements for the provision of the service.

A critical infrastructure organisation's senior executives should also be cognisant of the fact that many outsourced arrangements may rely on the use of sub-contractors for the delivery of components within the service in view. Where this occurs, contractual arrangements should ensure that the prime outsourcing provider remains accountable and responsible for all actions undertaken by sub-contractors, and are responsible for managing information security governance across all sub-contractors, providing assurance to the organisation.

Risk Management and Assessment

Effective risk management processes and detailed risk assessments are pivotal to the success of an outsourcing arrangement. Information security risk can be closely tied to other business risks, such as reputational or financial and as such, the importance of senior executives gaining a clear understanding of the relationship between information security risk and an organisation's overall corporate risk assessment cannot be understated.

In order to determine whether outsourcing services is suitable for an organisation, senior executives should satisfy themselves that a thorough risk assessment against the organisational objectives has been conducted using an appropriate methodology. It is also important to note that an organisation's risk landscape is rarely static and is highly likely to change over time. As a result of the fluidity that may underpin risk management, senior executives should ensure that a regular re-assessment of risks and associated mitigation strategies is conducted if an outsourcing arrangement has been established by the organisation, to ensure the risk landscape is accurate and up-to-date.

Change Management

Further to conducting effective risk management practices, large and complex contracts may require changes over their course. These changes may relate to information security, either through changes in the scope, functionality or performance of the outsourced services, or because the security requirement itself has changed. Senior executives should ensure that robust change management procedures are contractually agreed between the organisation and the outsourcing provider for any changes to the service which may have a material effect on information security.

Senior executives should also ensure that they have sufficient oversight and visibility into any material changes that occur within the arrangement that may impact the risk and information security posture of the organisation.

Assurance and Conformance

A key component of effective information security management, in an outsourcing environment, is the ability of an organisation to gain assurance that risks have been and will continue to be, effectively managed.

As a senior executive, it is vital that effective assurance mechanisms have been established within any outsourced arrangements. Without effective assurance mechanisms in place, senior executives and the organisation may be exposed to untreated risks in terms of overall business continuity, loss of reputation and/or regulatory non-compliance leading to financial loss.

Managing Information Security during the Outsourcing Process

Critical infrastructure provider senior executives will need to consider its in-house capability to effectively manage IT security throughout the duration of an outsourcing arrangement. If senior executives are not confident of its capability in this area, they may consider contracting this function to a qualified third party.

Incident Management

The actions taken in response to an information security breach or incident may have significant impacts on an organisation. As such, senior executives should satisfy themselves that outsourcing arrangements contractually oblige the outsourcing provider to report to a nominated contact within the organisation on an agreed basis (and format) all security related:

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

Termination and Transition

A contract can be terminated (discharged) or transitioned to alternative service provider for a number of reasons, including:

- the outsourcing provider fulfilling all obligations;
- mutual agreement;
- due to underperformance;
- a breach of contract; or

- as a matter of convenience[6].

Information security risks at this stage of the contract lifecycle may include:

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

Senior executives must ensure that the organisation has effective contractual and planning processes in place that manage the full range of information security risks during the termination or cessation of an existing contract or transition to a new contract and/or service provider.

4. Where to from here?

This supplement has only touched on the range of information security issues and planning considerations that a senior executive should be aware of when their organisation is considering the outsourcing of services. Further information is available in the complete guide available for download from the TISN website (www.tisn.gov.au).

It is recommended that senior executives use this supplement as a starting point, to commence the dialogue within their organisation, and to gain a greater understanding of the information security impacts and mitigations that may face their organisation.

As a result of thorough planning and consideration of the risks and issues surrounding the implementation of sound information security management principles, senior executives can make an informed decision on the suitability of outsourcing arrangements for their organisation and if outsourcing is deemed to be suitable, ensure that the appropriate controls and mechanisms are in place to effectively manage information security throughout the arrangements.

[6] *Developing and Managing Contracts, Getting the Right Outcome, Paying the Right Price*, ANAO Best Practice Guide, February 2007, p 100
www.anao.gov.au/