



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

Summary Report for CEOs and Boards of Directors

June 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.

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. Understanding an organisation’s IT security needs and ensuring that they are adequately reflected in contractual arrangements and managed through the contract lifecycle are critical elements of any outsourcing arrangement.

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. With critical infrastructure, IT failure can also have widespread national-security and social implications and cause considerable economic disruption.

The IT Security Expert Advisory Group¹ of the Trusted Information Sharing Network² has developed a resource, ‘Managing IT Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure’ (the Guide), which 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.

CEOs and Board members 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. 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 diligence³. Depending on the agreed terms of the contract, outsourcing transfers varying levels of management control, but it does not transfer compliance responsibility.

¹ 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.

² 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 or by contacting cip@ag.gov.au

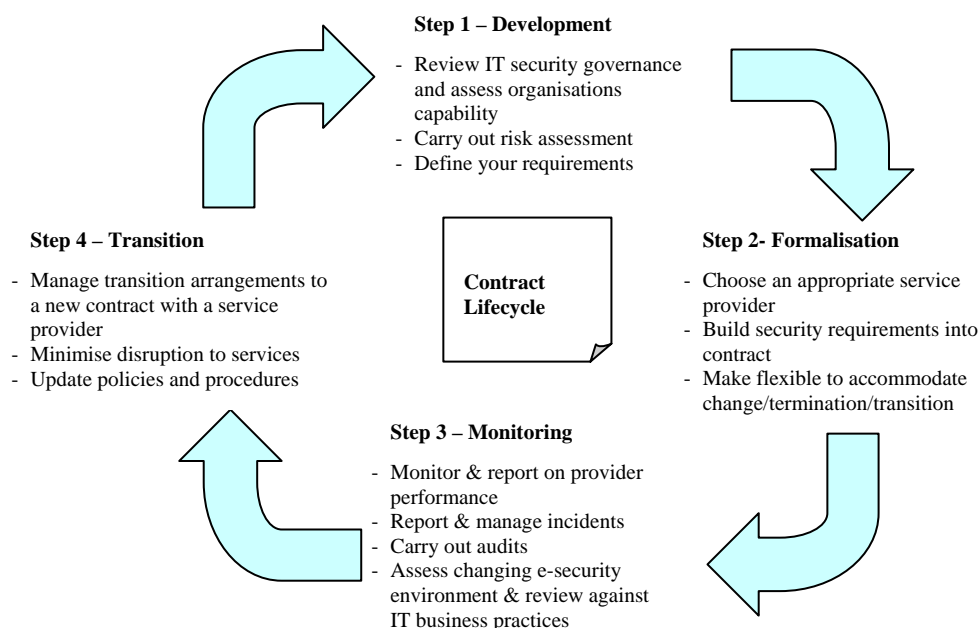
³ *Leading Practices and Guidelines for Enterprise Security Governance*, TISN, June 2006, p 43
www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Publications

Some of the pitfalls that could potentially befall an organisation in an IT outsourcing arrangement 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.

The guide provides a basic template for security in the contracting lifecycle.

Security in contracting lifecycle



The guide also suggests the need to have people on-hand with suitable IT security expertise to ensure that:

- the contract is properly managed;
- appropriate reporting, monitoring and auditing procedures are adhered to; and
- if something goes wrong, your staff and those of the service provider 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.

Questions you should be asking your CIO and procurement managers

- Have we completed a risk assessment of our IT functions to inform our negotiations with a service provider?

- What clauses in the contract protect our organisation's information and that of our customers?
- Does our contract contain clauses to strictly enforce monitoring, reporting and audit procedures?
- Do we have the IT security expertise on hand to assess IT security reports and properly manage any security incident—are these responsibilities within our organisation clearly assigned?
- Does our contract have the flexibility to accommodate changes in the IT security environment?
- Can we seamlessly and securely transition our IT functions to another service provider?

The complete version of the Guide is available at www.tisn.gov.au.

The 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.