



Australian Government

Department of Communications,
Information Technology and the Arts

Companion to
***A guide to limiting supplier liability in ICT contracts
with Australian Government agencies***



Companion to
***A guide to limiting supplier liability in ICT contracts
with Australian Government agencies***

August 2006

© 2006 Blake Dawson Waldron

ISBN 0 642 75365 2

Disclaimer

Except to the extent that a warranty is implied or right or remedy conferred on a person by an applicable law, the Department of Communications, Information Technology and the Arts, its officers, employees and contractors:

- (a) make no representation and give no warranty as to the accuracy of the information contained in this publication;
- (b) do not accept any responsibility for any error or inaccuracy in, or omission from, this publication (whether negligent or otherwise); and
- (c) are not liable for any loss or damage arising as a result of any person acting or refraining from acting on any recommendation or on the basis of any information contained in this publication.

What is this companion for?

This companion provides an introduction to key concepts and issues relevant to applying the Australian Government's Information and Communications Technology (ICT) liability policy.

A guide to limiting supplier liability in ICT contracts with Australian Government agencies (the guide) sets out in greater detail how to apply the ICT liability policy (refer to Finance Circular 2006/03 *Limited Liability in Information and Communications Technology Contracts*).

What is the ICT liability policy?

The ICT liability policy requires Australian Government agencies (agencies) subject to the *Financial Management and Accountability Act 1997* (FMA Act) to, in most cases, cap the liability of ICT suppliers at appropriate levels.

Standard agency contracts for the procurement of goods and services tend to have clauses that impose unlimited liability on the supplier. However, for ICT contracts, clauses imposing unlimited liability should only be included when there is a compelling reason.

The guide provides detailed assistance on implementing the policy. Model clauses that reflect the ICT liability policy will be set out in the SourceIT model contracts available at www.finance.gov.au/SourceIT

Who does the policy apply to?

The policy applies to all agencies subject to the FMA Act.

Commonwealth authorities and wholly-owned Commonwealth companies subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) are encouraged (where appropriate) to adopt procurement practices consistent with the policy and, where subject to section 47A of the CAC Act, can be directed by the Finance Minister to comply with the policy.

What goods and services does the policy apply to?

The policy applies to the purchase of all ICT goods and services, such as:

- hardware (e.g. personal computers, hard disks, keyboards, monitors, servers, modems and cables);
- software (e.g. operating systems, word processors, spreadsheets and databases);
- IT services (advice, analysis, development and support of IT infrastructure); and
- major office machines (e.g. printers, photocopiers, faxes, and electronic whiteboards).

The policy does not apply to goods and services procured under the Australian Government's Whole of Government Telecommunications Arrangements (WoGTA), which has its own liability regime.

What is a liability?

A liability is a legal obligation to pay or compensate another party. Parties usually allocate liability between each other in a contract. For example, in a typical contract an agency is liable to pay fees to the supplier, and the supplier is liable to compensate the agency for losses arising from breaches by the supplier of the terms of the contract.

Should all liabilities be capped?

It will not always be appropriate to cap all types of liability. While the final decision will ultimately depend on the particular circumstances, Figure 1 illustrates how to approach the decision on whether or not to cap different types of liability.

How and when should a cap be estimated?

To estimate an appropriate level for a cap, agencies will need to undertake a risk assessment. Risk assessment is part of risk management. Stages in a procurement process where risk assessments and considerations of capping liability may be required are shown in Figure 3 on page 6.

For high risk procurements, agencies may need to seek expert assistance.

Figure 1: Approaches to capping different types of liability

Type of liability	Usually cap	Maybe cap	Only cap if compelling reason
<ul style="list-style-type: none"> • Breach of the contract by the supplier • Negligence of the supplier 	<ul style="list-style-type: none"> ✓ ✓ 		
<ul style="list-style-type: none"> • Breach by the supplier of its intellectual property (IP) obligations • Breach by the supplier of its confidentiality and privacy obligations • Breach by the supplier of its security obligations 		<ul style="list-style-type: none"> ✓ ✓ ✓ 	
<ul style="list-style-type: none"> • Unlawful or wilfully wrongful act or omission of the supplier • Personal injury, sickness or death caused by the supplier • Damage to tangible property caused by the supplier 			<ul style="list-style-type: none"> ✓ ✓ ✓

What does a risk management/assessment process require?

A risk management process suitable for ICT procurement is summarised at Figure 4. Procurement officers should also refer to their agency's risk processes. Throughout the risk management process, procurement officers should regularly:

- consult and communicate with internal and external stakeholders; and
- monitor and review the risks and the risk assessment process.

An example of a simple risk analysis is at Figure 2.

What are qualitative terms?

In a general risk assessment, *qualitative* terms are used to describe the consequence and likelihood of the event occurring. For example, consequence may be assessed using a scale ranging from *insignificant* to *severe*, while for likelihood, a scale from *rare* to *almost certain* might be used.

What are quantitative terms?

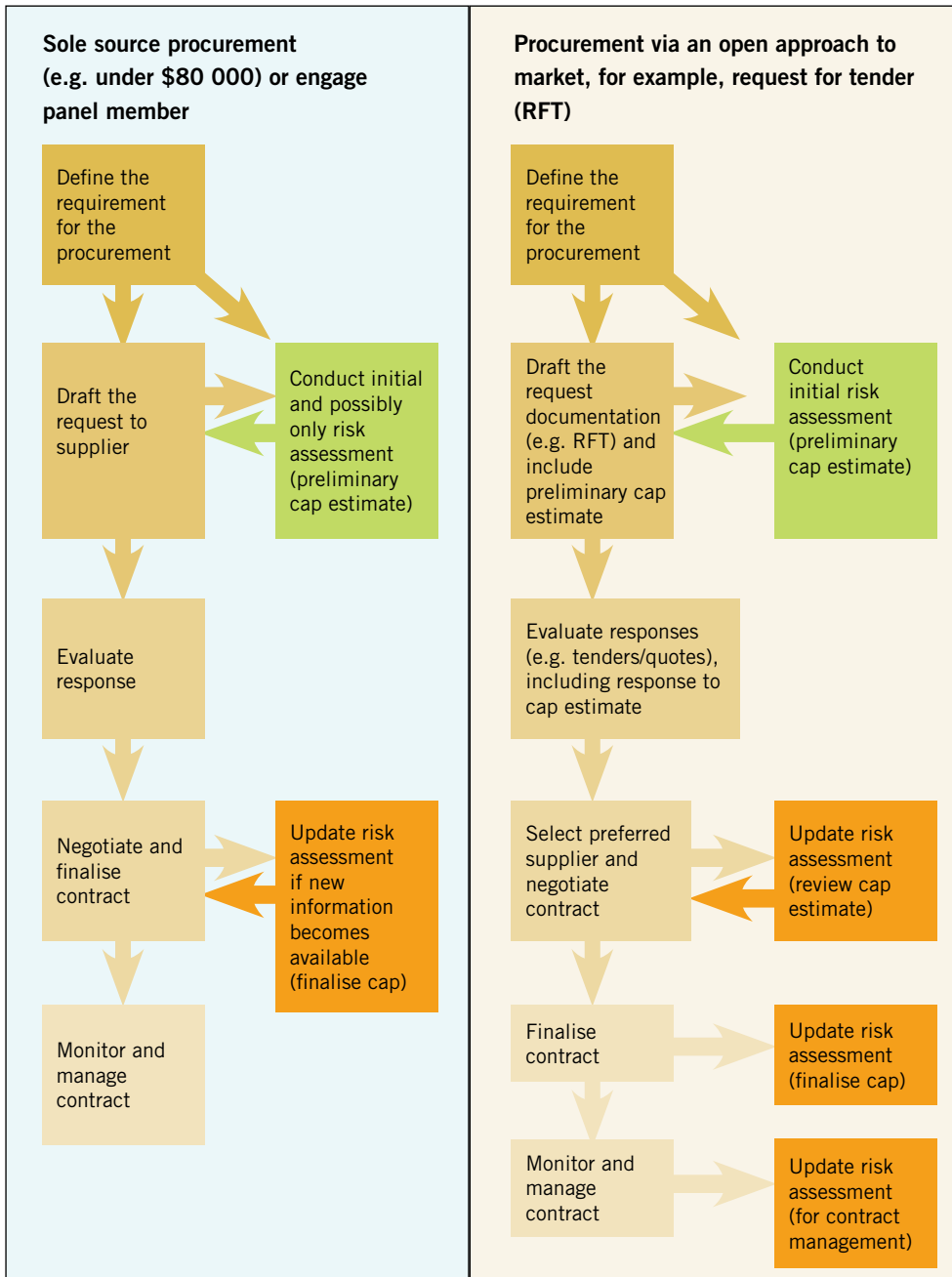
To estimate and allocate liability, *quantitative* (i.e. measurable) terms are used to describe *consequence* and *likelihood*. For example, consequence is usually described in dollars and likelihood as a numerical probability (e.g. 1 in 100 or 1 in 1 million).

Figure 2: Example of a simple risk analysis

An agency identifies a risk that a supplier might incorrectly install a power supply, causing damage to the ICT system. The risk assessment quantifies the value of the damage and the likelihood of that risk eventuating. For each risk that has been identified, the worst plausible financial consequences of the risk occurring are estimated to establish upper limits of liability.

Identified risk	Controls	Estimate	
The supplier might use inexperienced staff who fail to follow correct procedures and install an incorrect power supply in the system, causing severe damage to main circuit boards.	<ul style="list-style-type: none"> • Contract • Supplier experience • Built-in safety features 	Consequence	\$75 000
		Likelihood	1 in 1000
		Agreed liability cap (negligence)	\$75 000

Figure 3: Stages in procurement processes where risk assessments may occur



Case studies

The following case studies below provide examples of how to apply the ICT liability policy.

Case study 1: Procurement of wireless handheld devices (under \$80 000)

The agency is purchasing wireless handheld devices for its executive officers. A separate security risk assessment has been conducted and the use of these devices authorised.

Following consultation with its executive officers, the agency chooses a particular brand. An open approach to market is not required because the cost is expected to be less than \$80 000. The product can be purchased from an Endorsed Supplier under an Official Order issued under a Whole of Government Telecommunications Head Agreement (WoGTHA).

The procurement officer assesses the risks associated with the purchase and use of the devices. The key risks identified are poor product performance and damage to the agency's IT system arising from connection of the devices. The risk of product failure is considered moderate (1 in 100) and the risk of the devices causing damage is considered rare (1 in 10 000). The consequences of a risk eventuating are considered minor (equivalent to the value of the contract).

The agency issues the Official Order and, as no risks were identified to indicate the need for a higher level of liability, retains the default liability cap of \$50 000 under the WoGTHA Standard Contract Terms.

Case study 2: Hiring 20 IT contractors from an IT panel member

The agency has an urgent requirement to hire 20 IT contractors to work on the agency's IT service desk. The contractors will work with agency staff under agency supervision. An open approach to market is not required because of the panel arrangement. The agency has decided to approach a single member of its IT services panel to source the contractors. The panel arrangement stipulates that a risk assessment and liability arrangements will be determined at the time of placing a work order.

The agency issues a work order to the IT panel member requesting the provision of 20 IT contractors for six months at a price of \$600 000, based on the IT panel member's panel rates for the specified staff. The work order is issued under a standard panel contract.

The procurement officer undertakes an assessment of the risks associated with the performance of the services at the same time as drafting the work order. The risk assessment involves a brainstorming session attended by the procurement officer and the agency service desk manager and results in a risk register (see Appendix 9 of the guide).

The risk assessment supports the view that the procurement is low risk, primarily because the IT contractors would work under the supervision of the agency and are essentially required to work in accordance with agency-specified scripts (i.e. not in accordance with an untested service provider solution). The risk assessment also supports the view that, because of the safeguards and systems in place, the estimated damage arising from a negligent act or omission would be minor. In contrast, the possible damage arising from a malicious act that intentionally circumvented the safeguards and systems could be major. However, the risk of an IT contractor performing a malicious act is considered rare (1 in 10 000) because the work order requires all of the IT contractors to be security cleared, screened and experienced senior staff who have worked for the contractor for at least two years. The agency proposes a liability cap of \$100 000 based on an assessment of damage likely to arise from a negligent act or omission by the supplier. The cap does not apply to property damage, death, injury, security breach or damage arising from unlawful acts of the supplier, so liability is unlimited for these events.

Case study 3: RFT for the development and implementation of a new operational system

An agency needs to develop a management system that integrates a range of systems and technologies into a single source of information for use in highly critical, operational activities. As the agency estimates the cost to be about \$2.5 million, it prepares an RFT.

The procurement officer undertakes an initial risk assessment and produces a risk register at the time the RFT is being drafted. This involves several brainstorming sessions with a group of stakeholders including the project owner, system specialists and a number of agency IT officers. The initial risk assessment indicates that the procurement is potentially high risk and a risk assessment expert will need to provide assistance before the RFT is released.

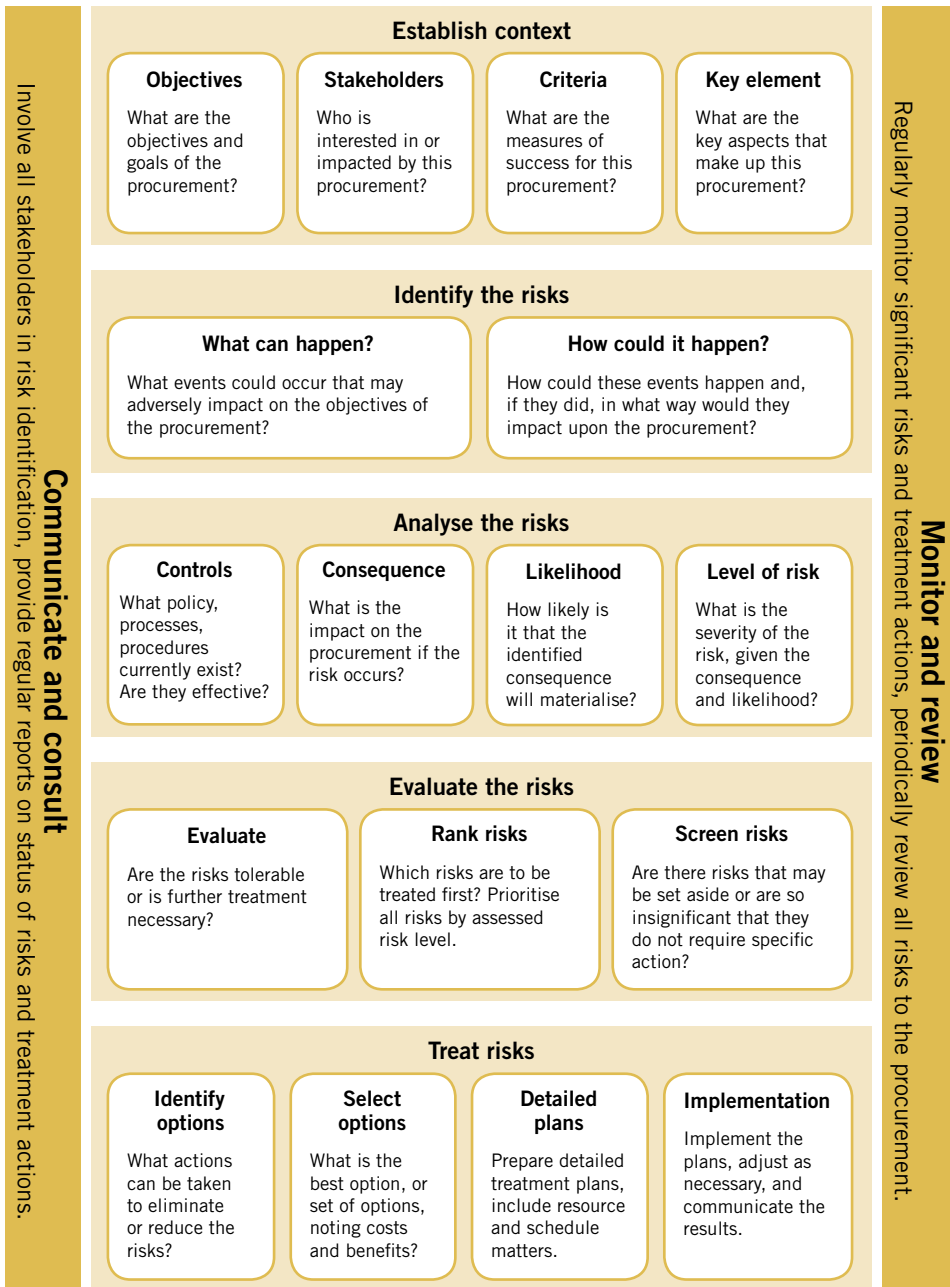
The expert conducts a workshop, which concludes that the impact of the new system failing is likely to be significant but hard to quantify. Input from stakeholders during the workshop suggests that licences to obtain and modify existing software would be difficult to obtain and could impede the contract if they were not obtained. However, the likelihood of the new system failing is assessed as unlikely (1 in 1000).

The risk assessment concludes that the direct cost to the agency of operational failure resulting from a system failure is not significant, but the consequential losses that the government might suffer as a result of the system failing (including claims by third parties for economic loss arising from business disruption while the system was down) would be severe, in the range of \$20 million.

The expert uses their own sophisticated risk modelling software to develop and simulate a number of models that address a range of possible risk scenarios and impacts. The models demonstrate with a 99.99 per cent degree of confidence that a liability cap of \$25 million will be sufficient to cover the financial impacts that the agency might face as a result of the contractor's actions.

Following the risk assessment, it was decided that a limit of supplier liability of \$25 million was appropriate, and this limit was included in the RFT and draft contract.

Figure 4: Standard risk management process



DEPARTMENT OF COMMUNICATIONS, INFORMATION TECHNOLOGY AND THE ARTS
www.dcita.gov.au