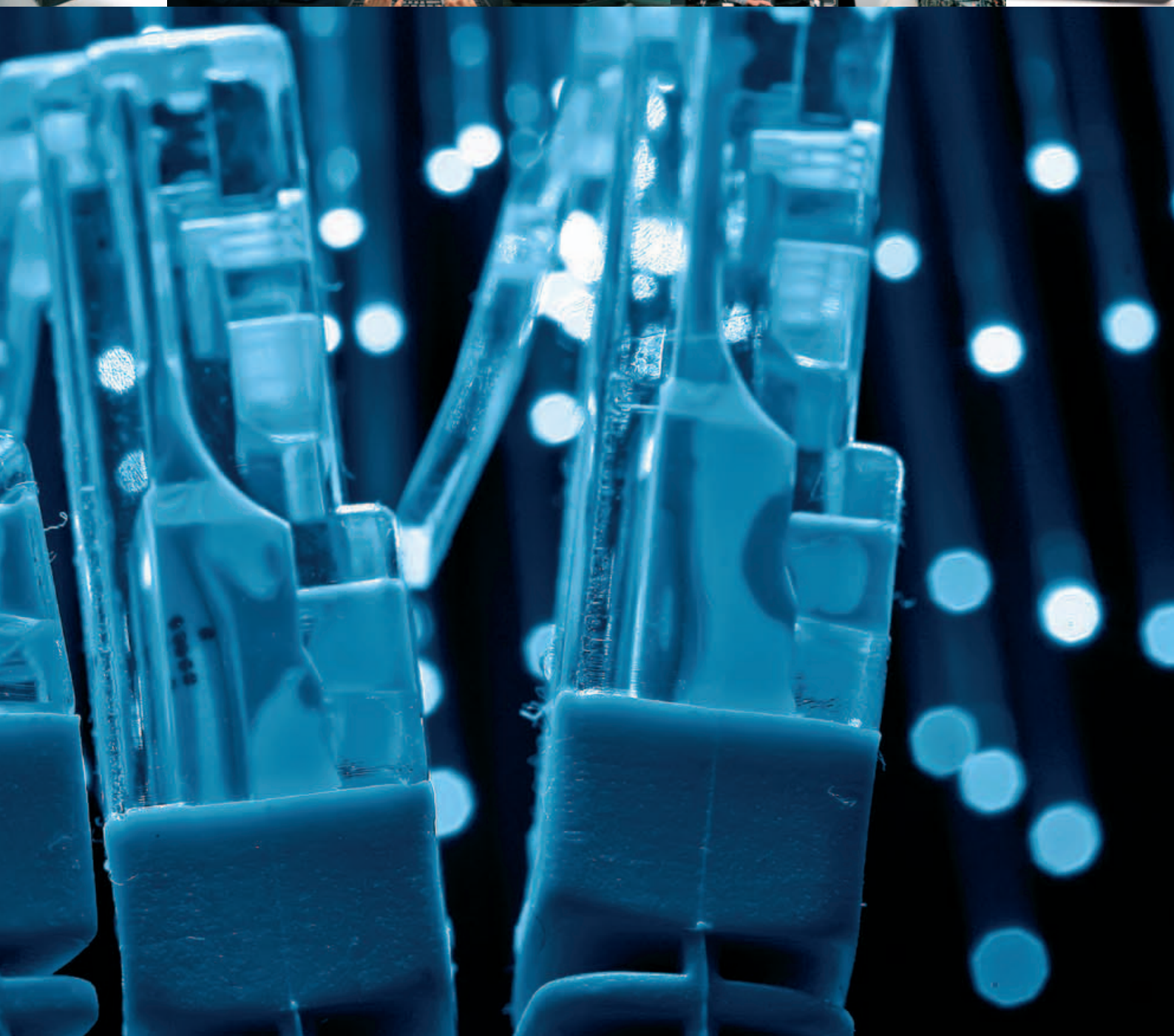
Australian Government

Department of Innovation
Industry, Science and Research

A GUIDE TO LIMITING SUPPLIER LIABILITY IN ICT CONTRACTS WITH AUSTRALIAN GOVERNMENT AGENCIES



A GUIDE TO LIMITING SUPPLIER LIABILITY IN ICT CONTRACTS WITH AUSTRALIAN GOVERNMENT AGENCIES

(Including developing and implementing risk assessment and risk treatment strategies)

Second Edition

MAY 2010

ISBN 978-0-642-72538-7

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 Innovation, Industry, Science and Research, its officers, employees and contractors:

- make no representation and give no warranty as to the accuracy of the information contained in this guide;
- do not accept any responsibility for any error or inaccuracy in, or omission from, this guide (whether negligent or otherwise); and
- 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 guide.

Information on the authors

Angela Summersby and **Andrew Davis** advise Australian Government agencies on outsourcing, tendering, market testing and procurement initiatives. They are part of Blake Dawson's specialist ICT team of legal advisors. Their contact details are:

Angela Summersby
Partner
Blake Dawson
Tel: + 61 2 6234 4024
angela.summersby@blakedawson.com
www.blakedawson.com

Andrew Davis
Senior Associate
Blake Dawson
Tel: + 61 2 6234 4029
andrew.davis@blakedawson.com
www.blakedawson.com

Phil Walker is part of **Broadleaf Capital International** (Broadleaf) a group of specialist consultants providing advice, facilitation and training in the areas of project risk management, strategic and enterprise risk management, procurement, contract management and negotiation, risk training, quantitative risk modelling and benchmarking. His contact details are:

Phil Walker
Associate Director
Broadleaf Capital International Pty Ltd
Tel: +61 412 708 305
Walker@Broadleaf.com.au
www.Broadleaf.com.au

INTRODUCTION

The Australian Government represents the largest information communications technology (ICT) market in Australia and winning Australian Government contracts is often a crucial part of the success and growth of many Australian ICT companies. It provides them with opportunities to develop innovative solutions and to obtain internationally recognisable references to support their export efforts.

The Australian Government's ICT liability policy recognises that requiring unlimited liability and inappropriately high levels of insurance can be a significant impediment to companies wishing to bid for Australian Government contracts. This is particularly so for small and medium sized ICT firms, which are not in a position to negotiate with their insurers.

Under the ICT liability policy, supplier liability should be limited in most cases in Australian Government ICT contracts, unless there is a compelling reason otherwise.

The first edition of this guide was published in August 2006 to provide detailed guidance on the application of the ICT liability policy, and was the product of extensive agency, industry and public consultation. In this second edition, the guide has been updated to reflect recent policy, commercial and legal developments, and to reflect agency experience in implementing the ICT policy since the first edition.

Agencies may need to monitor their implementation of the ICT liability policy in light of the finding in the Gershon Review[1] that, to date, the ICT liability policy has not been consistently implemented, resulting in either unlimited liability or limits on liability that are set at amounts that are so high that they are essentially the same as unlimited liability.

This guide reflects the Australian Government's support of the local ICT industry. This second edition continues to provide advice to help agencies and industry understand and work through what can sometimes be complex issues surrounding liability and risk management in ICT contracting. It includes a comprehensive risk management framework for agencies to follow in setting appropriate liability limits in ICT procurement contracts, and case studies to help illustrate the application of the ICT liability policy.

This risk based approach will generally reduce the liability coverage required in ICT contracts, decreasing the costs of tendering and doing business with the Australian Government, which should encourage greater participation and competition in the Australian Government ICT market.

1 Review of the Australian Government's use of Information and Communication Technology, August 2008.

CONTENTS

OVERVIEW OF THE ICT LIABILITY POLICY AND THE GUIDE

1. Introduction to the ICT liability policy

1.1 The Australian Government's ICT liability policy requires agencies subject to the *Financial Management and Accountability Act 1997* (the FMA Act) to, in most cases, limit ('cap') the liability of ICT suppliers at appropriate levels based on the outcomes of a risk assessment. Unlimited liability should only be required when there is a compelling reason.

1.2 The ICT liability policy was specifically developed by the Australian Government for ICT contracts to reflect the following particular characteristics of ICT procurement:

(a) always insisting on unlimited supplier liability may significantly reduce market competition, as many ICT suppliers, particularly small to medium enterprises (SMEs), are unwilling or unable to accept such liability;

(b) always insisting on unlimited or unjustifiably onerous supplier liability may result in agencies paying a higher than necessary contract price, as a supplier may include the cost of excessive insurance cover and their own risk premium in its price;

(c) the nature of some ICT development is inherently high risk, and an alliance-based or cooperative approach to sharing risk is sometimes necessary to find a supplier willing to undertake the work; and

(d) it is often difficult to identify the exact cause of a catastrophic ICT system failure, and hence where liability for such failure lies, particularly where there are more than two parties with interconnecting responsibilities.

1.3 The ICT liability policy is stated in Finance Circular 2006/03 *Limited Liability in Information and Communications Technology Contracts* (the ICT liability circular). A copy of the circular is included at **Appendix 2 – Finance Circular 2006/03.**

1.4 Key aspects of the ICT liability policy include:

(a) The starting position for an agency seeking to purchase ICT goods and/or services is:

(i) The agency should be prepared to limit the liability of its ICT supplier(s).

(ii) Each limit should be based on the outcome of a risk assessment.

(iii) The limit will be specified in a contract for ICT goods/services, and should only apply to damage or loss incurred in relation to that contract - it is an arrangement to limit a supplier's liability to compensate the agency, for damage or loss the agency incurs in relation to the contract.

(iv) The limit only applies to the parties to the contract – i.e. the agency and the supplier.

(v) The policy does not include agreeing to indemnity-type arrangements such as:

- limiting the supplier's liability to compensate a third party; or
- compensating the supplier for damage suffered directly by the supplier.

(i) The limit(s) would not normally apply to all categories of liability, such as liability for:

- damage to tangible property; (computer programs, software and data generally are not considered to be tangible property, and therefore the limit would normally apply to damage to software or data);
- personal injury;
- breach of intellectual property (IP) rights; or
- breach of obligations with respect to confidentiality, privacy and security,
- though limits should apply if there is a compelling reason to limit liability for any of those categories of liability.

(b) When approaching the market as part of a complex or high value procurement, agencies should, in the request documentation:

(i) include a draft contract with clear liability provisions;

(ii) require potential suppliers to:

- indicate compliance against each clause of the contract (including liability provisions);
- separately identify any clauses of non-compliance or partial compliance, and provide details and costs for any alternative clauses.

(c) When approaching the market agencies should also consider whether or not to:

(i) include in the proposal documents the level of the proposed cap and provide suppliers with the opportunity to propose alternative caps (and adjust their quoted prices accordingly); or

(ii) inform potential suppliers that, due to the nature of the procurement, liability will not be limited (an agency will need to justify a decision not to cap a supplier's liability in an ICT contract).

(d) The ICT liability policy must be applied in the context of the Australian Government's financial management framework. In particular, agencies must comply with the FMA Legislation (comprising the FMA Act, FMA Regulations and FMA Orders), the Australian Government's procurement policy framework and other financial management policies.

(e) Expert advice should be sought where necessary (e.g. due to the size, complexity or risk of the procurement).

2. Purpose of this guide

2.1 This guide is intended to help Australian Government agencies implement the ICT liability policy. The guide is also expected to assist those ICT suppliers that do business with the Australian Government to understand how agencies will implement the policy.

3. Procurements targeted by the guide

3.1 The diverse nature of contracts entered into by Australian Government agencies when procuring ICT goods and services means that it is not possible to provide a single approach to developing a risk management framework, conducting a risk assessment, and drafting liability clauses suitable for all ICT contracts. The guide does not mandate any one approach, but provides various examples of how agencies may implement the ICT liability policy.

3.2 This guide is particularly targeted to ICT procurements that can be described as low risk. Examples of *low risk* ICT procurements include:

(a) procurements that do not have the potential to severely or critically affect an agency's functions or service delivery if, for example, the supplier fails to deliver the goods and/or services on time, or if the goods and services delivered fail to meet the requirements under the contract;

(b) procurements of ICT components where the failure of those components will not severely or critically affect an agency's existing equipment or the development and delivery of high value infrastructure; and

(c) procurements of goods and/or services that are mature, tried and tested and have a proven track record of successful use without damage to the customer or third parties.

3.3 This guide also provides guidance on *medium risk* and *high risk* ICT procurements and describes a framework for undertaking risk assessments and determining liability caps suitable for such procurements. Medium or high risk ICT procurements might include one or more of the following characteristics:

(a) developmental software or hardware being integrated into complex and dependent systems;

(b) multiple layers of contractors and subcontractors providing services in a complex commercial and contractual framework; or

(c) an aggressive delivery schedule.

3.4 However, in the case of medium or high risk ICT procurements, agencies will need to undertake additional risk modelling to calculate the liability caps. In some cases, specialist risk assessment and legal advice may need to be sought, and unique liability clauses (possibly including several liability caps) will need to be drafted for inclusion in the contract. Agencies may also need to allocate additional resources for ongoing risk management.

3.5 Table 1 provides examples of procurements to highlight differences between low, medium and high risk procurements.

Table 1 - Examples of low, medium and high risk procurements

Examples of low risk procurements		
The supplier is required to undertake a scoping study of an agency's ICT user requirements. The main deliverable is an options paper. Development of any tools or processes (including testing) will occur under a subsequent procurement.	The supplier is required to deliver desktop equipment (e.g. PC, monitor, mouse, keyboard) ordered by the agency using its approved equipment catalogue.	The supplier is required to undertake the rollout of a hardware refresh (e.g. new PC, monitor, mouse and keyboard for each user).
Examples of medium risk procurements		
The supplier is required to undertake a data set standardisation project and develop a common platform for the submission of data across agencies.	The supplier is required to integrate a current, mature application into an agency's information management system.	The supplier is required to develop and implement a number of network support and administration tools across a large agency.
Examples of high risk procurements		
The supplier is undertaking applications development for the introduction of a new IT system, where the new IT system will: ■ replace existing reporting and processing procedures with one integrated IT system; and ■ have, as a key feature, improved security (e.g. public key infrastructure and encrypted transactions).	The supplier is required to provide IT support services to approximately 20,000 users. There are many points where the supplier's responsibilities and the agency's responsibilities interact.	The supplier is required to design and implement a new and very large network across an agency with numerous and disparate functions.

3.6 Procurement officers should note that there will not necessarily be any relationship between the cost of the proposed procurement and the risk to the agency. A low cost procurement may have the potential to cause a high level of damage to the agency, and conversely, a high cost procurement may be low risk and not have the potential to cause significant damage to the agency.

3.7 It is also important to recognise that a procurement initially considered to be a low risk ICT procurement may, following a risk assessment, subsequently be characterised as medium or high risk.

APPLYING THE ICT LIABILITY POLICY

A key finding of the Gershon Review is that the ICT liability policy has not been consistently implemented, resulting in either unlimited liability or limits on liability that are set at amounts that are so high that they are essentially the same as unlimited liability. This guide seeks to assist agencies to adopt a consistent approach to determining appropriate limits on ICT supplier liability based on the outcomes of a risk assessment.

4. Overview of approach to estimating appropriate limits on liability

4.1 Consistent with the CPGs[2], agencies should adopt best practice risk management strategies in estimating appropriate limits on a supplier's liability and managing risk. Each limit should reflect a properly considered estimate of the agency's risk arising from the proposed contract, and should not be arrived at arbitrarily. Estimating appropriate liability limits is one of the essential steps in determining value for money.

4.2 Estimating appropriate limits on a supplier's liability to determine value for money includes balancing the *consequence* and *likelihood* of the risk event occurring against the cost of treating the risk or insuring against it.

4.3 In assessing risk treatment and insurance costs, it is important to recognise that the supplier will usually factor into its price costs associated with the supplier bearing, treating or insuring against the occurrence of the risk. As the supplier's treatment and insurance costs are usually passed onto the agency, agencies will not necessarily obtain value for money by insisting that a supplier insure against all risks, no matter how remote.

4.4 Submissions to the Gershon Review highlight another risk to a procurement achieving value for money by indicating that requiring a supplier to bear unlimited liability can result in no bids and/or the offering of restricted solutions.

4.5 This guide describes the following four step approach for assessing risk and allocating liability.

1. Identify the risks that, if they were to eventuate, would cause damage to either the agency or the supplier.
2. Assess the likelihood of each risk (or a group of risks) eventuating, and for each risk (or group of risks), quantify the damage likely to be incurred if that risk were to eventuate.
3. Allocate, between the parties, liability (for the consequences of risks eventuating), taking into account:
   - Australian Government policy in relation to leaving specific types of liabilities uncapped (such as personal injury or death), unless otherwise justified;
   - the respective abilities of each party to manage or treat the risks; and
   - the costs associated with a party accepting liability.
4. Apply appropriate mechanisms to:
   - reduce the likelihood of the identified risks occurring (e.g. by undertaking security checks for supplier personnel); and

2 The CPGs state that "*If an agency decides to limit a contractor's liability, through a liability cap or indemnity, based on an assessment of the risks and value for money considerations, it should develop and implement a risk management plan*".

- treat the consequences (i.e. damage or loss) suffered if a risk eventuates (e.g. through insurance, backup procedures).

4.6 Officials should refer to their agency's Chief Executive's Instructions for information on any agency-specific procurement procedures and/or risk assessments.

5. To what goods and services does the ICT liability policy apply?

5.1 The ICT liability policy applies to the procurement by an agency of *information and communications technology*, which is defined in the policy as "*a term that encompasses the use of hardware, software and services to create, store, receive, transfer, process and present information*"[3]. This includes:

(a) Hardware – tangible, physical items such as personal computers, hard disks, keyboards, monitors and servers. Communications hardware includes modems, cables and ports;

(b) Software – programs that provide instructions on how an electronic device will operate. Examples of software include operating systems, word processors, spreadsheets and databases;

(c) ICT services – providing advice, analysis, development and support of ICT infrastructure. These services include ICT strategic planning, design and development of applications or networks and maintenance of ICT facilities; and

(d) Major office machines – printers, photocopiers, faxes, electronic whiteboards and multi-function devices.

5.2 The ICT liability policy does not apply to goods and services procured under the Australian Government Telecommunications Arrangements (AGTA), which is the mandatory framework for agencies procuring telecommunications *carriage* services (as defined by the *Telecommunications Act 1997* (Cth) and the preferred framework for acquisition of all other telecommunications related goods and services. AGTA has its own liability regime.

5.3 However, for *non-carriage* telecommunications that are not procured under AGTA, the ICT liability policy will apply. Agencies should refer to the Australian Government Information Management Office (AGIMO) website at www.finance.gov.au/agimo to confirm whether there have been any changes to that policy since the publication date of this guide.

5.4 Where an agency is considering procuring Microsoft products, it must now do so through the Australian Government's Volume Sourcing Arrangement (VSA) with Microsoft, which is mandated for use by all FMA Act agencies where they choose to purchase Microsoft products. The VSA is also available for use by CAC Act bodies (excluding Government Business Enterprises). The VSA is a contractual arrangement, and therefore terms such as the liability arrangements are already settled. As such, agencies will not be required to apply the ICT liability policy when procuring Microsoft products under the VSA. Further information on the Microsoft VSA may be found at http://www.finance.gov.au/procurement/ict-procurement/index.html or by contacting ictprocurement@finance.gov.au.

3 Finance Circular 2006/03 – Limited Liability in Information and Communications Technology Contracts.

6. Application of the ICT liability policy to shrinkwrap, clickwrap and web-wrap arrangements

6.1 It is important for agencies to be aware that ICT goods and services they purchase may often be subject to one or more of the following contractual arrangements.

(a) *Shrinkwrap* licences often accompany physically packaged software (e.g. on CD) and state that if the customer opens the packaging (usually plastic shrinkwrap, but may be any sealed package), the customer will be deemed to have accepted the terms of the licence dictated by the supplier.

(b) *Clickwrap* licences often apply to software downloaded by the customer and state that by clicking an '*I Accept'* or similar icon, the customer agrees to be bound by the licence terms dictated by the supplier.

(c) *Web-wrap* contracts are similar to a clickwrap licence, and contain the terms of access to a website, or perhaps the terms associated with the purchase of products from a website. Those terms are deemed to have been accepted by the user if an '*I Accept'* or similar icon is clicked.

6.2 Some of the key problems with these types of contractual arrangements are that:

(a) they are usually *take it* or *leave it* arrangements where the customer (in this case, the agency) has limited, if any, ability to negotiate or seek to amend the terms and conditions of the supplier's licence;

(b) the terms and conditions are often not clear as to their intended legal effect; and

(c) such licences are often accepted by agency users without regard to the agency's normal contracting position (including, for example, policies relating to the issue of indemnities by agencies).

6.3 Although there is limited ability for agencies to seek to amend the terms and conditions of shrinkwrap, clickwrap and web-wrap arrangements, agencies should only enter into such licences/contracts if the procurement is in accordance with the Australian Government procurement policy framework and the the ICT liability policy.

6.4 So, as a general rule, shrinkwrap, clickwrap and web-wrap licences/contracts should only be accepted by an agency if:

(a) the licence conditions have in fact been read by appropriately skilled procurement officers; and

(b) the agency forms the view that:

(i) any cap on the supplier's liability (which may be capped low or even exclude liability) is appropriate in light of the risks associated with the agency's use of the good or service; and

(ii) acceptance of the licence terms will not breach any other Australia Government procurement policy.

7. Interaction between the ICT liability policy and professional standards legislation

7.1 The Commonwealth, states and territories each have in place professional standards legislation[4] that provides a legislative upper limit on the liability of members of professions that have *approved* schemes. Under the legislation, occupational associations that represent people who work in the same profession or occupation (e.g. the Australian Computer Society (**ACS**) representing IT professionals) are able to prepare schemes (professional standards schemes) that are submitted to a professional standards council for approval. If the scheme is approved, members of that occupational association may then join the approved professional standards scheme and obtain the benefit of having their liability limited under that scheme.[5]

7.2 The key issue for agencies to be aware of is that under a professional standards scheme:

(a) a supplier may have its liability limited by the legislation;

(b) that limit may be lower than the limit the agency would propose be included in a contract with that supplier; and

(c) if the limit under the relevant scheme is lower than in the contract, the scheme limit will override the limit set down in a contract with the supplier, unless the supplier agrees to withdraw from the scheme.

7.3 It is important to understand that where a supplier has their liability limited under a scheme, the agency and supplier cannot contract out of this limit.[6] However, if a supplier is covered by a scheme, there is a legislative requirement that the supplier disclose its membership on all documents given to a client or prospective client that promotes or advertises the member or member's occupation, which would include tender documents and quotations. Failure to disclose is an offence for which there can be significant financial penalties, (up to $20,000). More importantly, a supplier that fails to disclose may not be able to use the scheme and obtain the benefit of the liability limit in the event of a claim.

7.4 The ACS has a scheme approved in NSW that, subject to mutual recognition provisions under their respective professional standards legislation, will apply in other Australian states and territories.[7] The scheme applies to ACS members who qualify as Certified Computer Professionals (CCP), a list of which will be published on the ACS website. This scheme commenced on 1 January 2010, and will expire on 31 December 2014.

7.5 Under the ACS scheme, occupational liability of CCP members of the ACS will be limited to $1.5 million. A member may apply to the ACS to specify a higher amount of liability than would otherwise apply under the scheme, up to a limit not exceeding $10 million. A member may also apply to the ACS to be exempted from the scheme. The proposed scheme will also require CCP members to have insurance for occupational liability of an amount not less than the amount of their limited liability.[8]

---

4 *Treasury Legislation Amendment (Professional Standards) Act 2004* (Cth) (which amended the relevant provisions of the following Commonwealth legislation: *Australian Securities and Investments Commission Act 2001*, *Corporations Act 2001* and *Trade Practices Act 1974*), *Professional Standards Act 1994* (NSW), *Professional Standards Act 2003* (Vic), *Professional Standards Act 2004* (SA), *Professional Standards Act 2005* (Tas), *Professional Standards Act 2004* (NT), *Professional Standards Act 1997* (WA), *Professional Standards Act 2004* (Qld), and *Civil Law (Wrongs) Act 2002* (ACT).

5 The legislation, generally, does not apply to liability for damages arising from (a) the death of, or personal injury to, a person; (b) a breach of trust; or (c) fraud or dishonesty.

6 For example, section 50 of the *Professional Standards Act 1994* (NSW), states: "This Act applies in relation to a person to whom a scheme in force under this Act applies despite any contract to the contrary...".

7 The scheme will operate in New South Wales, the Australian Capital Territory, the Northern Territory of Australia, Queensland and Victoria. The operation of the scheme in SA, Tasmania and WA will be dependent on the amendment of the law in those jurisdictions to allow interstate schemes to operate within their territory

8 Refer to the *Notification of Scheme (Professional Standards Act 1994 (NSW))* set out on the Professional Standards Council's website at www.lawlink.nsw.gov.au/psc.

7.6 Information on the progressive implementation of schemes in various jurisdictions (including the status of the ACS scheme) and the establishment of Professional Standards Councils in each jurisdiction can be obtained from the Professional Standards Council website www.lawlink.nsw.gov.au/psc.

7.7 It is important that agencies be aware of the existence of these schemes and seek legal advice before contracting with an organisation that is a member of a professional standards scheme, especially where the stated liability of the scheme is lower than, or inconsistent with, the liability arrangements developed by the agency after conducting its risk assessment. If an agency decides to contract with a member of a professional standards scheme, in addition to the issue of liability, the agency should also consider whether it requires insurance in excess of that required under the relevant scheme.

8. Interaction between the ICT liability policy and proportionate liability legislation

8.1 In addition to professional standards legislation, the Commonwealth, states and territories have also introduced proportionate liability legislation that, in general terms, limits the liability of a person to an amount reflecting the proportion of the loss or damage that person is responsible for. The proportionate liability legislation generally applies to claims for economic loss or damage to tangible property arising from failure to take reasonable care (eg to claims in negligence) or for misleading or deceptive conduct. The legislation does not apply to claims arising out of personal injury, or where the damage or loss is the result of the defendant's intended or fraudulent action.

8.2 Outside of the proportionate liability legislation, the general rule is that where two or more persons ('wrongdoers') are both held liable for a third party's loss, that third party could recover compensation for 100% of its loss from just one of those wrongdoers, notwithstanding that the other wrongdoer was also partly responsible for the loss.

8.3 Under the proportionate liability legislation, the third party may now only be able to recover as compensation from a wrongdoer an amount that is equivalent to that wrongdoer's share of responsibility for the loss.

For example

If person A suffers loss and:

- person X was held responsible for causing 70% of that loss; and
- person Y was held responsible for 30% of that loss,

person A can now only recover compensation for the amount of 70% from person X, and will have to pursue person Y for the remaining 30%.

Prior to the proportionate liability legislation person A could have recovered 100% from either person X or person Y.

8.4 The principal effect on agencies of the proportionate liability legislation is that it may limit a supplier's liability to an agency for claims involving purely financial loss or damage to tangible property, to an amount that a court determines reflects that supplier's responsibility for the loss or damage, notwithstanding that the supplier

and agency may have contractually agreed a higher cap, or no cap, on the supplier's liability for the relevant loss or damage.

8.5 Although the proportionate liability legislation introduced by each state and territory is similar, there are a number of important differences. One important difference is that in some jurisdictions, the legislation expressly allows parties to 'contract out' of proportionate liability[9], while in other jurisdictions the legislation is either silent on the question of contracting out, in which case it is not clear if contracting out is permitted, or contracting out is expressly not permitted. In those states where contracting out is allowed, agencies may include special provisions in their contracts[10] to ensure that the risk allocation and liability regime agreed by the agency and the supplier takes full effect. The ability to contract out of the legislation in some states and territories, but not others, may also impact on an agency's selection of the governing law for its contracts.

8.6 It is important that agencies are aware of the existence of proportionate liability legislation and seek legal advice on the potential operation and impact of the legislation for any ICT procurement that is identified by the agency as having a medium or high risk of loss or damage to the agency.

9. ICT liability policy and the Australian Government procurement policy framework

9.1 The ICT liability policy must be applied in the context of the Australian Government's financial management framework. In particular, agencies must comply with the FMA Legislation (comprising the FMA Act, FMA Regulations and FMA Orders (see sections 11 and 12 below)), the Australian Government's procurement policy framework and other financial management policies and particularly:

(a) the CPGs[11] (see this section 9 below);

(b) the ICT liability circular (ie *Finance Circular 2006/03 Limited Liability in Information and Communications Technology Contracts*);

(c) *Finance Circular 2003/02* and the accompanying *Financial Management Guidance No.6,* both titled *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort*; and

(d) *Finance Circular 2007/01 FMA Regulation 10* (see section 12 below); and

(e) *Finance Circular 2009/05 Commitments to spend money (FMA Regulations 7 to 13)*.

The Australian Government's procurement policy framework is described in detail at http://www.finance.gov.au.

9.2 In 2008, the CPGs were amended to explain more clearly that agencies should assess and manage risks for the purpose of considering appropriate limits (if any) on supplier liability. While the ICT liability policy dictates that agencies should limit liability unless there is a compelling reason not to, the CPGs are neutral as to whether or not it is appropriate to limit liability in other types of procurement and state "as a general principle, risks should be borne by the party best placed to manage them".

9 In NSW, WA and Tasmania the parties can contract out. Under the proportionate liability legislation of the Commonwealth, Victoria, ACT, SA and the NT, the legislation is silent on contracting out of proportionate liability. In Qld, the legislation expressly disallows contracting out.

10 For example, including a clause in the contract which expressly states that the relevant proportionate liability legislation does not apply to any claim between the agency and supplier.

11 Commonwealth Procurement Guidelines – 1 December 2008.

9.3 The CPGs set out the principles that apply generally to limiting a contractor's liability to the Commonwealth. For non-ICT procurements, the decision on whether or not to limit liability is to be made on a case-by-case basis, taking into consideration the outcome of a risk assessment, the direct and indirect costs associated with the liability position, and value for money impacts.

9.4 The CPGs explain the Australian Government's policy on contingent liabilities, which is to accept risk only where the expected benefits outweigh the costs[12]. The CPGs state that agencies should generally not accept risks which another party is better placed to manage. Similarly, where an agency is best-placed to manage a particular risk, it should not seek to inappropriately transfer that risk to a supplier.

9.5 Finance Circular 2007/01 requires agencies to treat as a contingent liability arrangements that limit a supplier's liability to meet costs that the Commonwealth may seek to recover from the supplier, where a third party has sued the Commonwealth for damage resulting from the supplier's action or inaction. Agencies may need to obtain FMA Regulation 10 authorisation before entering into a contingent liability, as discussed at section 12 below.

9.6 Consistent with the CPGs, implementation of the ICT liability policy requires agencies to undertake a risk assessment to analyse the:

(a) risks of liability arising;

(b) impact of such risks eventuating;

(c) appropriate level of any cap; and

(d) the potential costs of any liability cap.

9.7 When undertaking the risk assessment and determining the allocation of liability between the parties, agencies should note that the CPGs require agencies to consider the direct or indirect costs to the agency of agreeing to limit a supplier's liability through a liability cap when assessing value for money. Agencies should also note that the CPGs recommends that, for more complex procurements, request documentation should include a draft contract with clear liability provisions, require potential suppliers to indicate compliance against each clause of the draft contract, and clearly state and cost any alternative clauses. Request documentation may allow for any additional direct or indirect costs borne by the agency to be reflected in a commensurate adjustment to the terms of the contract where negotiations to limit a supplier's liability occur after the nomination of a preferred supplier.

10. Who must comply with the ICT liability policy?

10.1 The ICT liability policy applies to all agencies subject to the FMA Act.

10.2 Bodies subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) are legally and financially separate from the Commonwealth and are not generally required to comply with the ICT liability policy. Nevertheless, these agencies are encouraged, where appropriate, to adopt ICT procurement practices consistent with the policy. In addition, it should be noted that procurement officers of CAC Act bodies may be required to comply with the ICT liability policy in the following circumstances:

(a) where the CAC Act body decides (eg by a resolution of its directors) to comply with the ICT liability policy, and any relevant ICT procurement practices that are consistent with the policy;

12 Finance Circular 2003/02 and the accompanying Financial Management Guidance No. 6 (both titled Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort) set out the Government's policy on contingent liabilities.

(b) where the Minister for Finance and Deregulation (Finance Minister) has directed that CAC Act body to comply with the ICT liability policy and that CAC Act body is specified in the CAC Regulations for the purposes of section 47A of the CAC Act; or

(c) where the Finance Minister issues a General Policy Order under section 48A of the CAC Act that specifies the ICT liability policy as a general policy of the Australian Government applicable to that CAC Act body.

11. Complying with the FMA Legislation

11.1 The FMA Legislation sets out the law governing the proper use and management of public money and public property (that is, money and property in the custody or control of the Commonwealth, including money and property held by the Commonwealth on behalf of someone else, and money or property held by someone acting on the Commonwealth's behalf). The FMA Legislation establishes lines of accountability and reporting for FMA Act agency Chief Executives to their responsible Minister and, in some circumstances, to the Finance Minister.

11.2 Section 44 of the FMA Act sets out the obligations of Chief Executives with regards to complying with Australian government policy. Specifically, each Chief Executive is required to manage the affairs of the agency in a way that promotes "*proper use of the Commonwealth resources for which the Chief Executive is responsible*". In doing so, the Chief Executive must comply with the FMA Act, the FMA Regulations, Finance Minister's Orders, Special Instructions and any other law.

11.3 'Proper use' is defined to mean "*efficient, effective and ethical use that is not inconsistent with the policies of the Commonwealth*". Chief Executives must therefore manage the affairs of their agencies in a way that promotes ICT procurement which is not inconsistent with the ICT liability policy.[13]

12. Complying with the FMA Regulations

12.1 The FMA Regulations set down some specific requirements that must be complied with before entering into a contract, agreement or arrangement that gives effect to a spending proposal.

12.2 FMA Regulation 13 requires a person entering into a contract (or agreement or arrangement) under which public money is, or may become, payable to have approval under FMA Regulation 9, and if necessary, authorisation under FMA Regulation 10.

12.3 FMA Regulation 9 requires the approver of a spending proposal to be satisfied after reasonable inquiries that giving effect to the spending proposal would be a proper use of Commonwealth resources. Proper use means "*efficient, effective and ethical use that is not inconsistent with the policies of the Commonwealth*". An approver must therefore ensure that giving effect to the spending proposal would not be inconsistent with the ICT liability policy.

13 Where compliance with the requirements of the FMA regulations, Finance Minister's Orders, Special Instructions or any other law would hinder or prevent the 'proper use' of the Agency's resources, the Chief Executive must promote the proper use of those resources 'to the greatest extent practicable while complying with those requirements'

12.4 Where there is not sufficient uncommitted appropriation available to cover the maximum amount that would or could become payable under the spending proposal, FMA Regulation 10 requires an approver to obtain the written authorisation of the Finance Minister (or delegate) prior to approving that spending proposal.

125 Guidance as to when a spending proposal may require authorisation under FMA Regulation 10 is set out in *Finance Circular 2007/01 FMA Regulation 10* (**FMA Reg 10 Circular**). In particular, that Circular provides specific guidance in relation to spending proposals that contain a liability cap. Whether a spending proposal will require FMA Regulation 10 authorisation will depend on what is included in that cap.

12.6 For example, to comply with the FMA Reg 10 Circular in circumstances where an agency agrees to limit a supplier's liability in accordance with the ICT liability policy, FMA Regulation 10 authorisation:

(a) will generally **not** be required if the liability cap arrangements only limit a supplier's liability to the Commonwealth for damage the supplier directly causes the Commonwealth; but

(b) **will** generally be required if a contract limits a supplier's liability to meet costs that the Commonwealth may seek to recover from the supplier, where a third party has sued the Commonwealth for damage resulting from the supplier's action or inaction; and

(c) **may** also be required if the agency agrees to cap any indemnity from the supplier to the agency to the extent that indemnity includes such third party losses.

12.7 For completeness, it is worth noting that there are other arrangements that an agency might consider, that are outside of the ICT liability policy, for which FMA Regulation 10 authorisation will also generally be required such as indemnity-type arrangements that:

(a) limit a supplier's liability to a third party so that the Commonwealth is liable to the third party for any excess; or

(b) limit a supplier's exposure for damage the supplier has suffered itself so that the Commonwealth is liable to the supplier for any excess.

This is because these arrangements involve the Commonwealth agreeing to be liable for losses suffered by the supplier or a third party (see paragraph 13 of this guide for a discussion on the distinction between an indemnity and a liability cap). Such indemnity-type arrangements have generally been considered contingent liabilities for which FMA Regulation 10 authorisation would be required, and agencies should have regard to the relevant Australian Government policies before agreeing to indemnify a supplier.[14]

12.8 Agencies should seek assistance from the Department of Finance and Deregulation (Finance) if there is any uncertainty about FMA Regulation 10 in relation to liability caps. More details on the requirements of the FMA Regulations can be found at www.finance.gov.au. Agencies should also refer to the current *Financial Management and Accountability (Finance Minister to Chief Executives) Delegation* when considering whether the function or power of the Finance Minister to provide the required FMA Regulation 10 authorisation has been delegated to the agency's Chief Executive. Agencies may also need to consider obtaining legal advice to clarify the scope of a proposed liability cap.

14 See also paragraph 13 for a discussion on indemnities.

WHAT IS A LIABILITY AND WHAT IS A LIABILITY CAP?

13. Liability

13.1 A liability is a legal obligation to pay or compensate another party. Under a contract to procure ICT goods or services the parties will allocate liability between each other. For example:

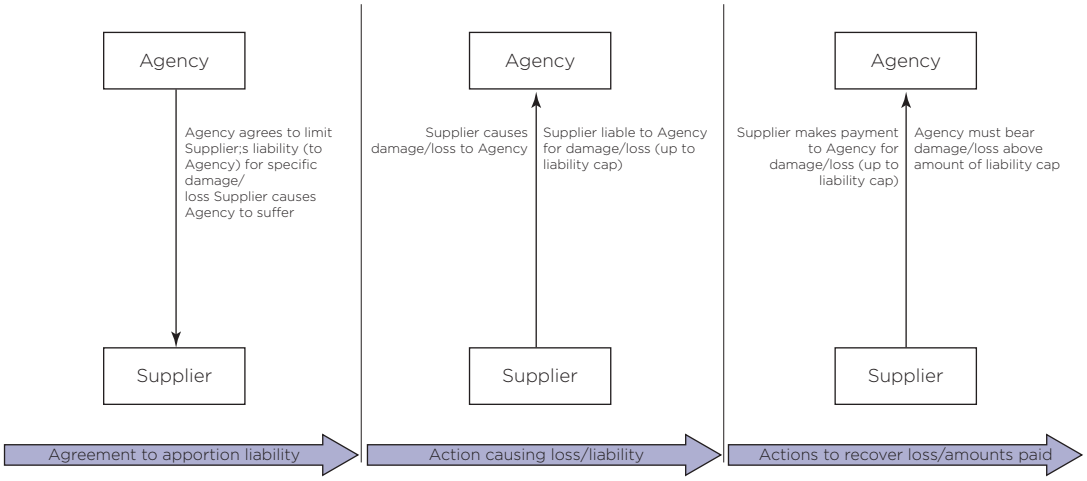
(a) the agency will agree to be liable to pay the supplier in return for the supplier providing the required goods or services under the contract;

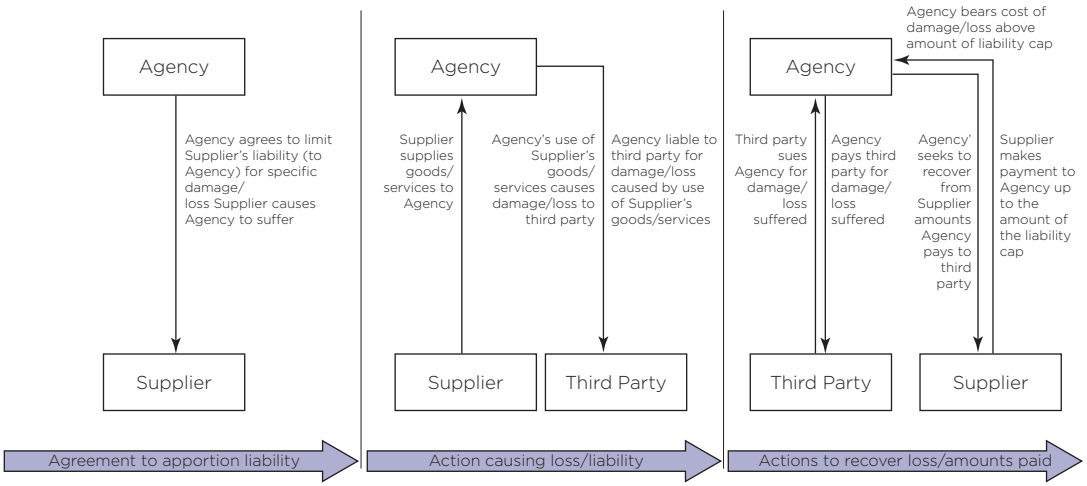
(b) the supplier will agree to be liable to the agency for the consequences of some events (e.g. the supplier accepts liability to pay for damage to the agency's tangible property caused by the supplier's negligent act or omissions in relation to the contract); and

(c) the agency and supplier may share liability for the consequences of some events.

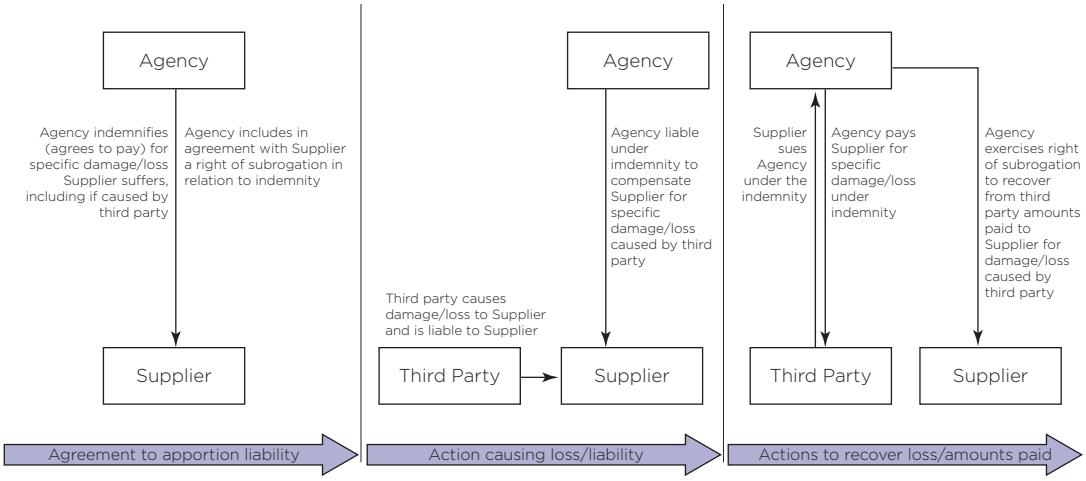
14. Liability caps and indemnities

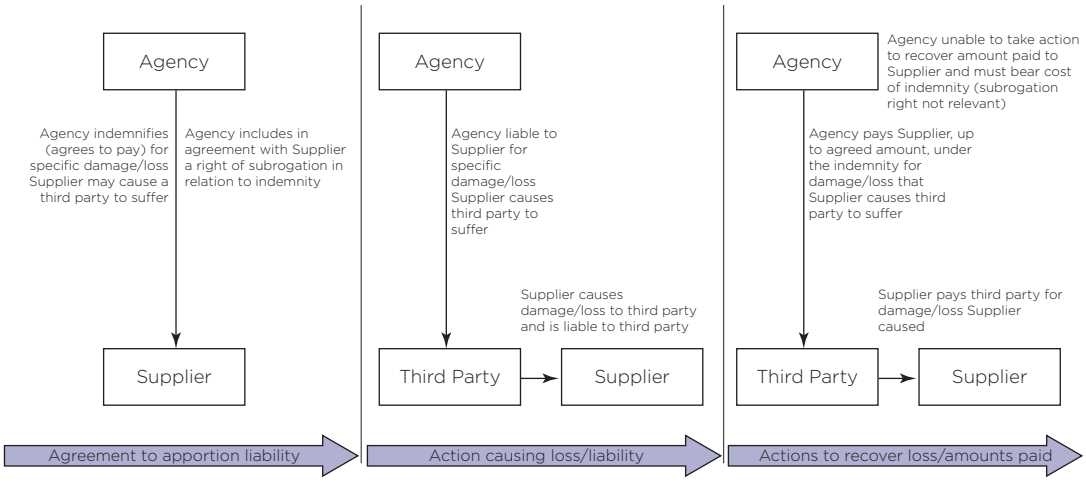
14.1 A common issue is understanding the difference between a liability cap and an indemnity. A liability cap is an arrangement where the first party (e.g. the agency) agrees to a limit on the liability of the second party (e.g. the supplier) *to the first party*. If the agency subsequently suffers a loss as a result of an act or omission of the supplier (in relation to the performance of the contract), the agency has agreed that it will not seek to recover from the supplier more than the amount of the agreed cap. Thus the risk of the agency suffering a loss caused by the supplier's act or omission will be shared by the supplier (up to the cap) and the agency (above the cap). Two common examples of liability capping arrangements are illustrated below.





14.2 An indemnity operates quite differently from a liability cap. An indemnity is an arrangement where the first party (e.g. the agency) agrees to accept the risk of loss or damage that the second party (e.g. the supplier) may suffer, whether or not the first party would otherwise be liable for that loss. Insurance is a common example of an indemnity arrangement where, in return for the payment of an insurance premium, an insurance company indemnifies (i.e. agrees to pay) the insured for losses the insured suffers (subject, of course, to various terms and conditions). If an agency agrees to indemnify a supplier, the agency is agreeing that if the supplier suffers a specified type of loss, the agency will meet the cost of that loss. An indemnity need not be unlimited – e.g. it may be activated only after the loss reaches a pre-agreed value, and/or it may be capped. Two examples of indemnity arrangements are illustrated below.





14.3 Most Australian Government contracts do not include an indemnity from the agency to the supplier.[15] Before agreeing to indemnify a supplier, agencies should have regard to the relevant Australian Government policies, in particular *Finance Circular 2003/02* and the accompanying *Financial Management Guidance No. 6* (both titled *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort*).

15. Categories of liability

15.1 There are a number of categories of liability. Subject to the exceptions listed in paragraph 15.3 below, the ICT liability policy supports capping, at appropriate levels, the supplier's liability (direct and indirect) arising from the following categories:

(a) liability for breach of contract; and

(b) liability for negligence.

15.2 There are certain standard Australian Government approaches (partly driven by policy objectives) to capping supplier liability that procurement officers should be aware of before agreeing to cap. These standard approaches are discussed below and procurement officers should seek legal or contract policy advice before departing from any of these approaches.

15.3 Australian Government contracts generally require that supplier liability not be limited for the following categories:

(a) liability for damage (direct and indirect) arising from a supplier's breach of its:

(i) IP obligations;

(ii) confidentiality obligations;

(iii) privacy obligations; and

(iv) security obligations;

(b) liability for damage (direct and indirect) arising from breach of any statute or any wilfully wrong act or omission;

(c) liability for loss of, or damage to, tangible property (covering both Commonwealth and third party property);

(d) liability for personal injury, including sickness and death; and

(e) liability for taxes (and any related penalties or interest) payable by the supplier or payable by the agency but recoverable from the supplier.

15 Many do, however, include an indemnity from the supplier to the agency - see for example, the indemnity provisions in the SourceIT model contracts.

15.4 In determining whether or not to cap supplier liability for any of the supplier activities or types of damage referred to in paragraph 15.3 above, procurement officers should have regard to the legal and policy reasons (discussed below) that underpin the tendency to not limit supplier liability for such activities/damage.

Liability arising from breaches of intellectual property obligations

15.5 There is no legal restriction on capping liability for breach of IP obligations. However, supplier liability is usually not limited because of the view that the supplier warranty of its right to provide IP is the equivalent of the standard warranty that the supplier of goods also pass good title to those goods. Legislation such as section 69 of the *Trade Practices Act 1974* (Cth) (which applies to consumer purchases, but nevertheless reflects the common law position) implies a warranty of good title in contracts for the supply of goods, and ensures that liability for failure to give good title cannot be limited or excluded. By analogy, liability for IP infringement in respect of ICT goods supplied by a contractor is similarly fundamental and should therefore not be excluded or limited.

Liability arising from breaches of confidentiality and privacy obligations

15.6 There is no legal restriction in Australia on capping liability for breach of privacy and confidentiality obligations. However, supplier liability is usually not limited because of the view that:

(a) the public should have confidence that the Australian Government will protect third party confidential information and personal information collected by or on behalf of the Australian Government—this confidence would be undermined if the Australian Government was to pass such information to suppliers whose liability in relation to their obligations to protect the information was capped;

(b) the Australian Government may have a moral obligation to at least advise those parties whose confidential information and personal information it collects, that it has capped the liability of suppliers dealing with that information in respect of the supplier's responsibility to protect the information; and

(c) limitations or exclusions of liability in ICT supply contracts for breaches of privacy and confidentiality interfere with the proper allocation of responsibility and implementation of responsible privacy and confidentiality principles, practices and protocols, as developed under regimes such as state and Commonwealth privacy and freedom of information legislation.

Liability arising from breaches of supplier security obligations

15.7 There is no legal restriction in Australia (or instruction in the Australian Government's Protective Security Manual) on the capping of liability for breach of a supplier's security obligations. However, the supplier's liability is usually not limited because, given the Australian Government's commitment to maintaining and enhancing security in relation to its operations, capping supplier liability in respect of security breaches would be inconsistent with, or dilute, that focus.

Liability arising from breach of statute or any wilfully wrong act or omission

15.8 The Australian Government does not usually agree to limit supplier liability for breach of any statute or any wilfully wrong act or omission because it is not considered appropriate to protect a supplier from the consequences of such acts or omissions. If an agency is considering limiting supplier liability for breach of any statute or any wilfully wrong act or omission, it should consider seeking guidance from the Department of Finance and Deregulation branch responsible for procurement policy.

Liability relating to any act or omission that constitutes repudiation of the contract

15.9 Repudiation is a legal concept that, in simple terms, refers to a party walking away from the contract. Repudiation is a wilfully wrong act or omission, and is expressly excluded from the liability cap in the SourceIT contracts to prevent a supplier 'abusing' their limited liability. For example, a supplier might decide during the contract that, due to a change in the market (e.g. a significant increase in the prices it can charge due to a shortage of supply) it is profitable to walk away from the contract. This is because the profit it could make from diverting its resources into newer, more lucrative, contracts would exceed the damages it would have to pay for breaching its contract with the agency, as those damages would be capped.

Personal injury, sickness and death

15.10 There is no blanket legal restriction in Australia on the capping of liability for personal injury, sickness or death, although some legislation prevents contracting out of statutory imposed liability in relation to certain types of personal injury and death[16]. However, supplier liability is normally not limited for this type of event because the Australian Government's preference is not to place a value (e.g. the amount of the liability cap) on personal injury or death that may arise in relation to a contract. Also, a supplier is usually able to obtain appropriate insurance (such as public liability, product liability and professional indemnity insurance) at commercially acceptable premiums to cover its unlimited liabilities for these types of event.

Damage to tangible property

15.11 There are valid commercial reasons for agencies not agreeing to cap supplier liability for damage to tangible property caused by the supplier, and it is common practice in both public and private sector ICT contracts to not limit liability for such damage including because:

(a) if the agency caps the supplier's liability, the agency's building and contents insurance usually will not cover the agency for damage above the cap[17]. Building and contents insurance is one of the few insurances that an agency will hold that covers, among other things, damage that might be caused by a supplier (agencies are unable to insure against most other types of damage caused by a supplier—for further explanation see the section on insurance at section 30); and

(b) if an agency is able to insure against such loss, it should not negate that insurance without a compelling reason.

Liability for tax

15.12 There is no policy that supports limiting the liability of the supplier to pay taxes (Commonwealth or state) arising in connection with ICT contracts. It is therefore prudent to take care to ensure that the liability of the supplier to pay taxes is not inadvertently limited by the limitation of liability clause. This should not generally be an issue where standard form agreements are used, as these usually have appropriate tax clauses, such as the GST clauses in the SourceIT model contracts. However, legal advice should be sought before tax clauses are amended.[18]

16 For example, the Trade Practices Act 1974 (Cth) voids attempts by corporate manufacturers and importers to contract out of liability where an individual suffers injury as a result of a defective good.

17 The Comcover standard policy provides cover for loss, destruction or damage to an insured agency's tangible property, but does not automatically cover contractually assumed risks (such as a liability cap), and an agency may be uninsured for liability above the liability cap. Insurance issues are discussed in greater detail at sections 30 to 33.

18 SourceIT does not include tax clauses for all situations, and depending on the nature of the services being procured, agencies may need to consider including additional clauses, such as in relation to withholding tax and employment tax.

CAPPING LIABILITY

16. The SourceIT liability capping clauses

16.1 Model clauses that reflect the ICT Liability Policy approach to capping supplier liability are set out in the SourceIT model contracts available at www.finance.gov.au. Agency contracts may also have their own standard liability clauses. Procurement officers should not amend model or standard clauses without a compelling reason before departing from, or negotiating changes to, model or standard clauses (including any definitions of loss). Procurement officers should consider seeking legal advice and take into account the costs, including on suppliers, in having to consider the potential effect of clauses that deviate from the standard clauses.

16.2 As the SourceIT User Notes do not explain the operation of the liability clause, an example clause from the SourceIT model Hardware contract (version 2.0) is set out below, with an explanation of each of the issues that the clause is seeking to address.

Table 2 - Source IT liability clause.

Clause (SourceIT, Hardware, 2.0)	Comment
32.2 Limitation *(a) The liability of each party arising out of or in connection with this Contract (including under any indemnity) is, subject to clause 32.2(b), limited to the amount specified in item 30 of the Contract Details.*	It is sound commercial practice for agencies to seek to have their own liability limited, especially when agreeing to limit the liability of the supplier. The default position should therefore be that limit on liability is mutual (ie both the contractor and the Commonwealth should obtain the benefit of the limit). The amount specified as the limit in the Contract Details should be expressed as being "exclusive of GST".
(b) Unless specified otherwise in item 31 of the Contract Details, any limit on the liability of each party under clause 32.2(a) does not apply in relation to liability relating to:	In general, it will be appropriate for exclusions from the limit on liability to also be mutual, subject to one notable exception – 'repudiation' – as described below. Agencies should carefully consider the effect, and obtain appropriate legal advice, before modifying any of the exclusions set out below.
(i) personal injury (including sickness and death);	Personal injury will usually be excluded from any limit on liability.
(ii) loss of, or damage to, tangible property;	Loss of, or damage to, tangible property will usually be excluded from any limit on liability.
(iii) an infringement of Intellectual Property Rights;	Infringements of Intellectual Property Rights will usually be excluded from any limit on liability.
(iv) a breach of any obligation of confidentiality, security matter or privacy; or	Breaches of any obligation of confidentiality, security matter or privacy will usually be excluded from any limit on liability.
(v) any breach of any statute or any wilfully wrong act or omission including, in the case of the Contractor, any act or omission that constitutes repudiation of the Contract.	Breach of any statute or any wilfully wrong act or omission will usually be excluded from any limit on liability. Repudiation of the contract by the Contractor should be expressly excluded from any limit on its liability. Repudiation is a legal concept that, in simple terms, refers to a party walking away from the contract. In that situation, the Contractor should not obtain the benefit of any limit on liability that is set out in the contract that the Contractor is walking away from. The 'repudiation' exclusion should not apply to the Commonwealth as this could have the effect of being inconsistent with the Commonwealth's right to terminate a contract 'for convenience' – eg where there is a change of government or government policy.
(c) Unless specified otherwise in item 32 of the Contract Details, the limitation of liability specified in clause 32.2(a) applies in respect of each single occurrence or a series of related occurrences arising from a single cause.	The default position is for the limit on liability to apply to any one event (or interrelated events), with no aggregate limit on liability. However, there will be situations where an aggregate limit on a supplier's liability will be appropriate. For a SourceIT contract, an aggregate limit will need to be expressly stated in the Contract Details.
32.3 Review of limitation *(a) The parties acknowledge that the limitation of liability specified in item 30 of the Contract Details will be subject to review in the event that the Contract is varied or extended.* *(b) For the avoidance of doubt, a party may require a review of the limitation of liability specified in clause 32.2 as a condition of its acceptance to a variation request under clause 21, but only for the purpose of achieving a proportionate adjustment to reflect any alteration to that party's risk exposure arising out of that variation.*	It is important to review any limit of liability where there is any variation or extension to the contract as these events can alter the risk profile on which the original limit was based.

17. Negotiating the liability cap clauses

17.1 There are a number of commercial issues that procurement officers should have regard to when seeking to negotiate liability capping clauses.

Fixing monetary value of the cap(s)

17.2 Generally the amount of a liability cap will be a fixed dollar figure, although attempts may be made to tie the cap to the contract sum or some multiple of the contract sum. Agencies should avoid the practice of tying the amount of a cap to the contract value, or any multiple of that value, as the level of risk of a procurement may have no relation to the price of the contract.

17.3 That is not to say that the level of risk will never have a connection with the price of goods being purchased. Where the contract is solely for the delivery and/or installation of goods (hardware or software), there is always a risk that some or all of those goods (including installation) may not be fit for the purpose for which they have been supplied, and/or do not meet the specifications for which the supplier has warranted.[19] Where the goods are not fit for purpose or do not meet the required specifications, the goods are likely to be of little or no value to the agency and will need to be replaced. In that situation it may be appropriate to ensure that the supplier is liable for at least the full cost of replacing those supplies either by:

(a) setting a liability cap that is no lower than the cost of replacing the hardware (and depending on the full range of risks identified in the risk assessment, as discussed below, the cap may be higher); or

(b) including a provision in the contract to impose an obligation on the supplier to replace, at the supplier's cost, goods that are not fit for purpose, and amending the liability clauses to exclude from the liability cap this obligation on the supplier to replace the goods.

17.4 Unlike a contract for goods, the minimum level of supplier liability in a contract (or part of a contract) for services would not generally have a connection with the price of the services being purchased. Services are not generally a 'one-off' delivery, but involve a series of ongoing deliveries. Accordingly, an agency can terminate the services part-way through the contract and engage an alternative service provider if the services fail to meet the standards required by the contract. There are, of course, other risks that may flow from inadequate service delivery that would be identified during the risk assessment and that will be important for setting the appropriate level of liability.

17.5 Agencies should be wary, and seek legal advice, before agreeing to cap a supplier's liability at the amount that may be recovered from the supplier's insurance. This type of cap introduces additional risk for the agency as the agency's ability to recover will be reliant on:

(a) the detailed terms and conditions of the supplier's insurance policy (and any exclusions set out in that policy); and

(b) the supplier complying with the terms of the policies, so as not to void the insurance.

This type of cap can also lead to a total exclusion of liability where, for example, the terms of the policy limit the amount payable to the supplier's legal liability (which may be nil due to the circularity of linking the supplier's liability to the insurance policy).

19 SourceIT, for example includes a number of warranties, such as 'be fit for the purpose as set out in the Statement of Work'.

17.6 The only way to properly determine an appropriate amount for a liability cap is through the conduct of a risk assessment.

'Per event' or 'aggregate' cap?

17.7 A per event cap (also known as per occurrence cap) means the cap only applies to a single occurrence, or series of related occurrences, arising from a single cause. For example, if the cap is $100 000 per event, then the supplier's liability for each single event is capped at $100 000, but its total potential liability is likely to greatly exceed $100 000 (i.e. its total potential liability is $100 000 multiplied by the number of events that cause the agency damage or loss).

17.8 An aggregate cap, in contrast, is a cap on the supplier's total liability, irrespective of the number of events that occur. An aggregate cap might be stated to apply for the term of the contract, or for a specified period such as a financial year. For example, the cap might be $300 000 in aggregate each financial year, so that the supplier's liability for each financial year will be capped at $300 000, no matter how many events occur that cause the agency damage or loss. Under this example, for a contract that spans three financial years, the supplier's maximum liability under the contract would be up to $900 000. Alternatively, the supplier's liability might be capped at $600 000 in aggregate for the term of the contract, and while the supplier's maximum liability under the contract would then be up to $600 000 it would also be liable for up to $600 000 in any one year (contrasted with the per year cap referred to above).

17.9 While a per event cap is more likely to cover all damage caused by a supplier under a contract, there may often be compelling reasons to consider an aggregate cap. Specifically, a per event cap does not enable suppliers to understand or calculate their total liability under the contract, and hence price the commercial risk of entering into that contract. An aggregate limit, on the other hand, makes it easier for the supplier to estimate its total liability under the contract, and can be agreed to where such a limit is supported by an appropriate risk assessment. When negotiating an aggregate cap it is important to remember that:

(a) an aggregate cap should reflect (or include an assessment of) the number of events that a supplier might cause that lead to losses during the contract term, taking into account the identified treatment strategies to reduce the risk of a loss-causing event reoccurring;

(b) the risk assessment should result in both per event and aggregate caps to cover all possible negotiated outcomes (otherwise a risk assessment for a per event cap may need to be reviewed/adjusted to arrive at an appropriate aggregate cap); and

(c) if the aggregate cap is exhausted early in the contract term, then the incentive on the supplier's part to manage risk is reduced, though where the loss relates to a breach of contract, the agency should have included a right to terminate for breach, and in lieu of exercising that right may be able to renegotiate the liability cap[20].

17.10 In some cases, the parties will negotiate the inclusion of both per event caps and an aggregate cap. If an aggregate cap is included in the contract, it should be higher than all of the per event caps (e.g. $2 million per event, with a $4 million aggregate cap).

20 Further, in many Commonwealth contracts agencies will require a right to terminate for convenience for any reason.

GST and the limit of liability

17.11 The amount specified to be the limit of liability should be expressed as a GST exclusive amount. Agencies should confirm that appropriate GST clauses, such as those found in SourceIT model contracts, are included in their standard contracts to allow them to recover an additional amount from the supplier on account of GST.

17.12 For example, the SourceIT model contracts provide for the limitation of liability amount to be specified in the Contract Details. When specifying that amount, agencies should specify that the amount is exclusive of GST. The effect may be, for example, that while the supplier's liability may be specified to be limited to '$1million exclusive of GST', if GST were to be payable in relation to the loss or damage suffered by the Agency, the supplier may be liable to pay the Agency $1million plus GST – i.e. up to $1,100,000 under the GST 'gross-up' clause in the SourceIT contract. The supplier may then be able to claim back the GST component of $100,000 from the Australian Tax Office as a GST input tax credit, provided it holds a valid tax invoice.

Review of liability cap upon contract extension

17.13 Agencies should reassess the risk assessments, review the liability cap and if necessary, negotiate an amendment to the cap before:

(a) each option to extend the contract is exercised; or

(b) the contract is varied in any material way.

Mutuality of capping

17.14 Ideally agencies should seek to negotiate mutual limits on liability where appropriate — that is, not only should the supplier's liability to the agency be capped, but also the agency's liability to the supplier should be capped. However, the amount of each cap will not necessarily be the same for each party as each cap should reflect the specific risks to which each party is exposed under the contract, and the extent to which each party is able to manage and treat those risks.

Exclusion of 'indirect' or 'consequential' losses

17.15 It is common for a supplier to seek to have its liability in relation to 'consequential' or 'indirect' losses not just limited under the contract, but excluded altogether. It is important to note that an exclusion of liability operates independently of, and in addition to, a limit on liability. The effect of such an exclusion is to relieve the supplier of all liability for the types of loss to which the exclusion applies. Therefore considerable care needs to be exercised when considering whether or not to agree to an exclusion of liability.

17.16 Where an exclusion of liability relates to 'consequential loss' or 'indirect loss', there are additional issues to consider, especially as the scope of these terms remain uncertain in Australian law. At the time of publication of this second edition of the guide, the most recent case law suggests that the term 'consequential loss' may be interpreted broadly. Accordingly, if an agency were to agree to completely exclude a supplier's liability for 'consequential loss', and the majority of losses likely to be suffered could be characterised as 'consequential losses', the liability cap may be of little importance as the supplier would have little liability to limit.

17.17 To avoid this uncertainty, agencies should avoid use of the terms 'consequential loss' and 'indirect loss', and instead request a supplier to identify the specific events and types of loss for which it is seeking to limit its liability for (eg 'loss of profit'). This is the approach adopted in the template liability clauses for SourceIT, which do not refer to 'consequential loss' or 'indirect loss'.

17.18 When considering an exclusion for 'consequential loss' or 'indirect loss', agencies should consider the following issues:

(a) Is it clear what damages the supplier regards as being indirect or consequential losses? The agency may wish to consider whether these types of losses should be defined in the contract to ensure the exclusion of liability is not greater than the agency intends;

(b) Does the risk assessment support a conclusion that the supplier should not be liable for such *indirect* or *consequential* losses?; and

(c) Has the supplier justified why it should not be liable for such *indirect* or *consequential* losses, noting that a general cap on liability has been offered?

18. Other liability related clauses and issues

18.1 Capping liability is only one of many approaches to allocating liability under a contract, and liability caps should not be considered in isolation from the other clauses in the contract that allocate liability. Clauses that a supplier may seek to amend include those set out below.

Performance clauses

18.2 The performance or delivery clauses — these impose an obligation on the supplier to perform, and a failure to perform will result in the supplier being liable to the agency for breach of contract. These clauses are essentially in the form of:

the supplier will perform the services specified or described in the statement of work.

18.3 Suppliers often try to reduce their liability to perform the services described in the statement of work by seeking contractual provisions that make the supplier's obligation to perform to a certain level conditional on the agency providing inputs to the product being developed or service being delivered. While these clauses will be reasonable in many procurements, procurement officers need to understand the impacts and limits on the supplier's obligations if agency inputs are not delivered on time and at the required quality.

Liquidated damages

18.4 Liquidated damages clauses are often included to compensate the agency for specific types of breach by the supplier, such as delay, late delivery, unavailability of a service or other such underperformance by the supplier.[21] A key feature of liquidated damages is it removes the requirement for the agency to measure and quantify its *actual* losses. The amount of liquidated damages payable by a supplier for underperformance is pre-agreed and described in the contract as either a rate (eg $1 000 for each day that a service is unavailable) or a specific amount.

18.5 As a general rule, to enforce a liquidated damages clause the rate or amount of liquidated damages must not be a penalty, but must instead be a *genuine* pre-estimate (decided at the time of making the contract) of the loss or damage that the "injured" party is expected to suffer as a consequence of the breach by the supplier. Importantly, the liquidated damages will be a penalty, and therefore not enforceable, if the amount of the liquidated damages is "extravagant and unconscionable" compared with the loss that could be proved to have followed from the breach.

21 SourceIT does not include a clause for "liquidated damages", but does include provision for service rebates to be applied. Service rebates operate much like liquidated damages where they are a genuine pre-estimate of damages likely to be suffered by the agency as a result of a breach or failure by the supplier.

18.6 For government contracts, however, the Australian courts have recognised that there is an inherent difficulty in pre-estimating an agency's loss in relation to a potential breach by the supplier (and hence in determining an appropriate amount of liquidated damages). Nevertheless, the courts have acknowledged the appropriateness of including liquidated damages in government contracts.

18.7 Accordingly, a liquidated damages clause in an agency's contract should be enforceable (not a penalty) even where there is difficultly in pre-estimating an agency's likely loss, or where it is not possible to base the amount on a precise or accurate calculation, so long as the amount of the liquidated damages is not extravagant and unconscionable in comparison with the greatest loss that could conceivably be proved to have followed from the breach. Nevertheless, agencies should consider documenting the method used to calculate the amount of the liquidated damages to assist in demonstrating that the amounts are not "extravagant and unconscionable".

18.8 Generally no GST will apply to the payment of an amount by one party to the other by way of liquidated damages in the context of a genuine dispute. However, in case GST does apply, it is important that the ICT contract does not limit the ability of either party to recover GST on payments for damages or for other claims.

Warranty clauses

18.9 Warranty clauses—these are where one party warrants it will deliver a certain result and is liable if that result does not eventuate. These clauses are essentially in the form of:

> *the supplier warrants that during the warranty period, each service and good will conform with the specifications.*

18.10 Procurement officers should be wary of a supplier using the warranty clause to actually limit the supplier's liability. This can occur where, for example, the supplier amends, or adds to, a standard warranty (such as that in the SourceIT model contracts) to specify things that the supplier 'does not warrant'. In such cases, the supplier has limited its liability to provide a good or service to a standard that the agency might otherwise have expected. Shrinkwrap, clickwrap and web-wrap licences/contracts are particularly likely to include statements as to what the supplier does not warrant.

Exclusion clauses

18.11 Exclusion clauses — sometimes referred to as "force majeure", "unavoidable delay", "excusable delay" or in SourceIT as "unforeseen events" - relieves either party from liability for a failure to fulfil its obligations under the contract in certain defined circumstances (e.g. bad weather, accidents, etc). In SourceIT, the relevant clause is:

> *A party (Affected Party) is excused from performing its obligations under this Contract to the extent it is prevented by circumstances beyond its reasonable control (other than lack of funds for any reason or any strike, lockout and labour disputes in respect of the Contractor only), including but not limited to acts of God, natural disasters, acts of war, riots and strikes outside that party's organisation.*

RISK MANAGEMENT AND RISK ASSESSMENT PROCESS

19. Overview

19.1 The process for estimating an appropriate level of supplier liability under a contract requires an assessment of the risks relating to the proposed contract (the risk assessment process). Specifically, an assessment must be made of:

(a) risks that could cause damage to either party (if the risks eventuate);

(b) the extent to which the agency considers those risks would be best managed by the supplier (and the extent to which liability for those risks should be transferred to the supplier in the contract); and

(c) the extent to which the agency is willing to accept liability, from a policy perspective, in relation to those risks (including by capping the supplier's liability to the agency in the contract).

19.2 The risk assessment process is part of a broader risk management process (see Figure 1).

19.3 Most agencies are expected to adopt an approach to risk management based on the new risk management standard: Australian/New Zealand AS/NZS ISO 31000:2009 Risk management - Principles and guidelines, 2009 (released in November 2009). The new standard is supported by ISO Guide 73, which provides the definitions of terms related to risk management, as well as ISO/IEC 31010 which provide an overview of risk assessment techniques.

19.4 The risk management standard provides a generic guide for managing risk, and defines risk as the "*effect of uncertainty on objectives*". Comcover has also declared that the new standard is suitable to be considered by agencies when developing and implementing their approach to managing risk.

19.5 Consistent with the risk management standard, agencies use this approach to risk management in order to:

(a) Increase the likelihood of achieving objectives;

(b) Encourage proactive management;

(c) Be aware of the need to identify and treat risk throughout the organisation;

(d) Improve the identification of opportunities and threats;

(e) Comply with relevant legal and regulatory requirements and international norms;

(f) Improve financial reporting;

(g) Improve governance;

(h) Improve stakeholder confidence and trust;

(i) Establish a reliable basis for decision making and planning;

(j) Improve controls;

(k) Effectively allocate and use resources for risk treatment;

(l) Improve operational effectiveness and efficiency;

(m) Enhance health and safety performance, as well as environmental protection;

(n) Improve loss prevention and incident management;

(o) Minimise losses;

(p) Improve organisational learning; and

(q) Improve organisational resilience.

More information on the risk management standard can be found at the Standards Australia website www.standards.org.au and the Comcover mainpage www.finance.gov.au/comcover.

19.6 The risk management process described in the risk management standard involves five steps:

(a) establish the context;

(b) identify the risks;

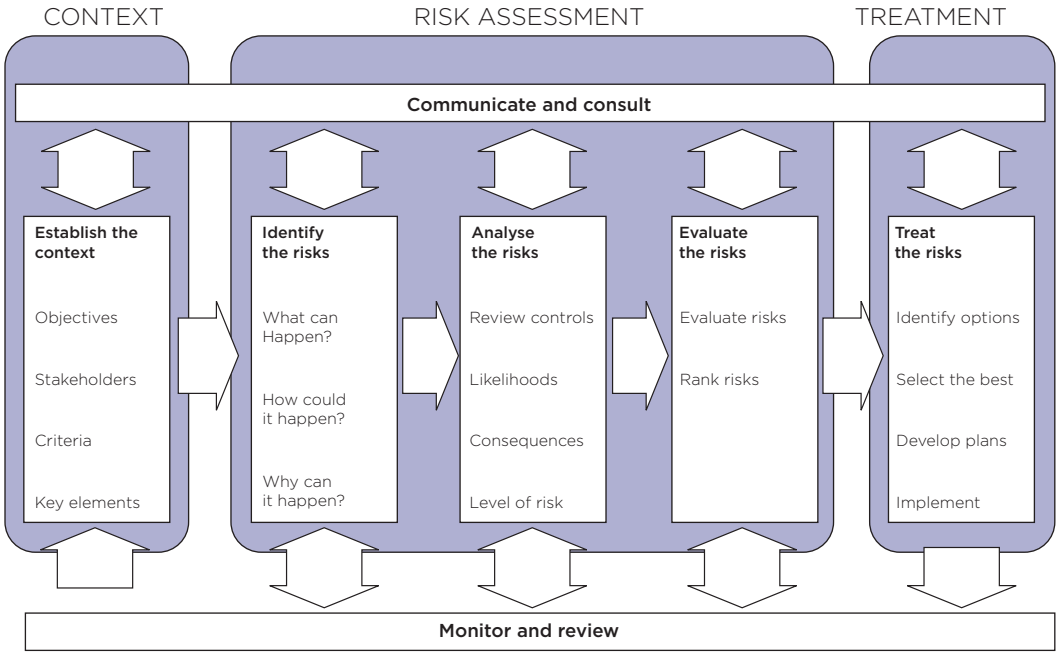
(c) analyse the risks;

(d) evaluate the risks; and

(e) treat the risks.

19.7 Throughout the process, there should be consultation and communication with internal and external stakeholders, and ongoing monitoring and review of the effectiveness of each step. Figure 1 illustrates the process.

Figure 1 - Risk management process



19.8 While this guide provides a general overview of the risk management and assessment process, procurement officers should be aware of their agency's own particular risk management processes.

20. Step 1: Context - establish the context of the risk assessment

20.1 The first step in the risk management process is to establish the context for the risk assessment. In a procurement for ICT goods/services, the context involves understanding the background of the agency and its objectives in undertaking the procurement.

20.2 There are a number of elements to establishing the context. These are:

(a) defining the objectives of the contract/procurement, the nature of the contract and its limits, and the agency'

(b) identifying the stakeholders (internal and external to the procurement) who are affected by or who are able to influence the contract/procurement;

(c) clarifying the scope of the goods and services to be delivered, including the key elements of those goods and services; and

(d) identifying the criteria for measuring the risk consistent with the objectives of the procurement.

20.3 Establishing the context is important to maximise the efficiency, accuracy and completeness of the risk assessment process and to direct the risk identification step and detailed assessment activities that follow.

20.4 It is possible to define the context for a procurement by developing a context statement, drawing together the aspects that make up the context of the procurement. An example of a simple context statement for an ICT contract is shown in **Table 3**.

Table 3: Example context statement

Context part	Description
Objectives	■ The contract provides for the supply of two mainframe computers and support for a period of ten years for the agency. ■ The mainframes will need to be installed and operational within six months and the price is not to exceed the approved allocations within the agency's budget.
Stakeholders	■ Agency procurement area ■ End users within the agency ■ The Minister
Environment	■ External - business, regulatory, financial and political environment ■ Internal - culture, structure, internal stakeholders.
Criteria	■ Technical performance ■ Financial ■ Delivery schedule
Key elements	■ Design ■ Manufacture ■ Installation and check-out tests ■ Operation ■ Maintenance and support

21. Step 2: Risk Identification

21.1 The second step in the risk management process (and the first step in the risk assessment process as illustrated in Figure 1 above) is to identify the risks related to the delivery of the goods/services under the proposed contract — that is, what events might occur that could impede fulfilment of the contract by either party?

21.2 The risk identification step has a number of parts. It involves identifying:

(a) the potential risks under the contract (i.e. what might happen and what might be the effects on the objectives of the contract);

(b) how, when, where and why those risks might occur; and

(c) the impact of those risks and who they might affect.

21.3 Risk identification is crucial to risk assessment—unidentified risks cannot be assessed and treated. Therefore it is very important that the risk identification process is comprehensive. The process should be structured using the key elements developed as part of the context step to systematically examine the risks in each area of the contract.

21.4 Information used in the risk identification process may include historical data, theoretical analysis, empirical data and analysis, informed opinions of experts and the concerns of stakeholders.

21.5 A useful approach to identifying risks is brainstorming in a group workshop. This is a little more demanding on participants than the use of superficially attractive mechanisms such as checklists, but it is significantly more effective. Brainstorming allows the risk identification process to draw on the creative capacity of the participants, reducing the danger of overlooking new and emerging issues. In comparison, checklists tend to be static and fixed at a particular point in time.

21.6 The selection of participants for a brainstorming workshop is very important. They should be chosen to include expertise that covers all areas of interest for the procurement. This may include stakeholders who stand to be impacted by acts or omissions by the supplier, and people external to the agency.

21.7 The end product of the risk identification process should be a comprehensive list of all risks associated with the contract that may lead to one party suffering damage and the other party being liable for that damage. Risks should be described in sufficient detail to reduce the potential for the nature of the risk to be misinterpreted.

21.8 An example of a description of a risk, as might be developed during the risk identification process, is as follows.

> The supplier may use inexperienced staff or fail to follow correct procedures and install an incorrect power supply in the client system, leading to severe damage to main circuit boards.

22. Step 3: Risk Analysis

22.1 Once the potential risks have been identified, the next step is to conduct a risk analysis to better understand the severity of the risk. A risk is analysed by estimating and combining the consequences and the likelihood of the risk occurring. The results of the risk analysis should be documented, and will usually be included in a risk register (refer to **Appendix 8 – Example risk register**).

22.2 A risk analysis may be straightforward or quite complex, depending on the procurement activity. Risk analysis has a number of clear steps, including:

(a) evaluating the effectiveness of existing controls;

(b) determining the consequences flowing from the risk eventuating;

(c) determining the likelihood of the risk eventuating; and

(d) using the consequence and likelihood ratings to determine an overall level of severity for each risk.

Controls

22.3 Analysis of identified risks must fully consider existing risk controls. A risk control treats an identified risk to some extent. Controls are often found in existing policy, processes and procedures. Risk analysis often relates to how effective the existing controls are in treating a risk.

22.4 Existing controls that may be in place for the example risk mentioned at paragraph 21.8 include:

(a) detailed specifications in the contract;

(b) supplier experience in similar contracts and/or pre-qualification for the services; and

(c) built-in safety design features of the system.

Consequences

22.5 Consequence ratings are generally described in qualitative terms, that is, using words to describe the relative impact of the event occurring. A qualitative assessment of consequence might involve a five-point descriptive scale, ranging from 'insignificant' to 'severe'. Consequences are to be considered in terms of the potential impact on the criteria developed during the context stage (refer to **Appendix 6—Qualitative measures of consequence and likelihood**).

22.6 For the purpose of estimating and allocating liability under the contract, the consequence of the risk (should it eventuate) needs to also be quantified. That is, the consequence of a risk occurring is expressed in monetary terms.

Likelihood

22.7 A qualitative assessment of likelihood can also be described in terms that reflect a similar five-point descriptive scale, ranging from a likelihood described as 'rare' to one described as 'almost certain' (refer to **Appendix 6—Qualitative measures of consequence and likelihood**).

22.8 Where complex risk modelling is employed, a quantitative approach to allocating and estimating liability under the contract is necessary.

229 Quantitative assessments of likelihood are usually expressed as a probability in powers of ten. For example, a risk may have a one in a thousand or one in ten chance of occurring. In complex risk modelling, quantitative assessments like this are important measures against which liability limits may be estimated.

22.10 Assessments of likelihood must consider:

(a) the effectiveness of any existing controls; and

(b) the probability that a risk will occur (given any existing controls).

22.11 The accuracy of an assessment of likelihood depends on the accuracy and detail of the information available and the knowledge and experience of those participating in the brainstorming session. Participants need to draw on their experience when assessing likelihood, and base their assessments on this experience. They should also call upon any empirical data, statistics, history, anecdotal evidence that may be available, and any other relevant sources when making an assessment.

22.12 Where workshop participants are at odds over the likelihood of a risk occurring, it is preferable that the most pessimistic estimate of likelihood (i.e. a likelihood of one in ten, rather than one in a hundred) be accepted. This ensures that there is some level of confidence and margin for error in the final estimate of liability limits.

1.1 Risk analysis example

A procurement officer identifies a risk that the proposed supplier may install an incorrect power supply into a system, leading to damage to that system. The risk assessment should quantify the value of the damage, and the likelihood or probability of that risk eventuating. For each risk that has been identified, the financial consequences of the risk occurring should be estimated, using the worst plausible financial consequence. This is because the purpose of the risk assessment is to establish upper limits of liability.

22.13 The example in **Table 4** illustrates the kind of detail that needs to be captured during the risk identification and risk analysis stages.

Table 4: Example risk analysis

Risk number	Risk description	Controls	Financial consequence (worst case)	Likelihood
1	Supplier may use inexperienced staff who fail to follow correct procedures and install an incorrect power supply in the system, leading to severe damage to main circuit boards.	Detailed specifications in contract. Supplier experience in similar contracts. Built-in safety features of the system.	$75 000	1 in 1000

23. Step 4: Risk Assessment - evaluate the risks

23.1 The risk evaluation step is a decision making step in the risk assessment process. Based on the risk analysis, decisions need to be made about:

(a) whether risks are acceptable at their current severity level or require risk treatment strategies to be developed to reduce the severity; and

(b) the priority for treating those risks assessed as capable of and requiring treatment.

23.2 Risk evaluation has a number of parts, including:

(a) evaluation of the risks;

(b) ranking of the risks; and

(c) screening of minor risks.

23.3 During the risk evaluation, the initial identification and analysis results are reviewed against the stated context information, especially the criteria used to make decisions, to ensure consistency and accuracy. Adjustments are to be made to consequence and likelihood assessments as required, and risks that have no bearing on the objectives of the contract and risk assessment can be put aside for the moment (refer to **Appendix 6—Qualitative measures of consequence and likelihood**).

23.4 The end product of the risk evaluation stage is a complete set of risks, with details of controls, consequence and likelihood, validated for relevance, accuracy and significance and prioritised for treatment.

24. Step 5: Risk Treatment

24.1 Treatment of the risks has a number of elements, including:

(a) identification of the options to treat the identified risks;

(b) assessing and selecting the preferred risk treatment options; and

(c) developing and implementing plans to treat the risks.

24.2 When following the risk management process set out in the risk management standard, strategies for treating the identified risks are developed once the assessment of the risks has been completed – i.e. after risk identification, analysis and evaluation.

24.3 Risk treatment involves identifying options for treating the risks, assessing the options, and selecting those options that are considered to be the most effective at reducing the severity of the risk. An assessment of the options involves comparing the costs of implementing each option against the potential benefits associated with that implementation. The preferred options are expanded in detail, responsible officers are allocated the task of managing the risks, and treatment strategies are implemented.

24.4 Again, using a brainstorming workshop or group of experienced staff to develop treatment options is the most effective way of identifying and evaluating strategies to treat unacceptable risks. A diverse group of people will put forward a range of possible solutions to the risks, and provide a balanced view in deriving a final risk treatment strategy.

24.5 There may be a number of measures included in a contract to treat risk, such as the inclusion of detailed specifications, a formal test and acceptance regime, and requirements for formal skill levels and competencies for supplier staff and implementing additional internal agency procedures to manage the procurement.

24.6 When allocating liability under the contract, the options are not merely limited to a choice of either agreeing to limit supplier liability or insisting on unlimited liability. If liability is to be limited, then there will usually be a number of options as to how to decide on an appropriate limit. There may also be a number of other measures included in a contract to treat risk, such as the inclusion of detailed specifications, a formal test and acceptance regime, and requirements for formal skill levels and competencies for supplier staff. In addition to allocating liability under the contract there may also be other options to treat risks, such as implementing additional internal agency procedures to manage the procurement.

24.7 Treatment strategies may take the form of specific provisions in the contract or may include actions that fall outside of the contract framework. For example, the contract may include specific provisions for the acceptance of deliverables in response to an identified risk. Outside the contract, the agency may have identified a risk relating to their ability to effectively manage the contract with the supplier, and so the preferred treatment strategy may be the recruitment of a technical specialist to assist in managing the contract and supplier.

24.8 Responsibility for managing a particular risk should fall to the party best able to manage it. With respect to the delivery of the goods/services, this may, though not always, be the supplier.

249 In addition to allocating and limiting liability in the contract, other contractual measures can also be used to reduce the likelihood and/or consequence of a risk. By reducing the overall severity of the risks, the level of liability the supplier will be required to accept in the contract may also be reduced. As a result of effective risk management processes, the costs for both the supplier and the agency may be reduced.

For example, in the scenario referred to in **Table 4**, paragraph 22.13, the procurement officer may decide that a reasonable treatment strategy, additional to the existing controls, would be for the supplier to conduct a series of installation tests and checks before installing the new power supply on the system. This additional work would not reduce the consequences if the installation was undertaken incorrectly, but may reduce the likelihood of the risk occurring from, for example, a likelihood of one in a thousand, to a one in ten thousand likelihood. This, in turn, may result in a lower limit of supplier liability.

24.10 **Table 5** shows how adding further treatment strategies may reduce the likelihood of the risk occurring.

Table 5: Example risk analysis (with additional risk treatment)

Risk number	Risk description	Controls	Additional risk treatment	Financial consequence (worst case)	Likelihood
1	Supplier may use inexperienced staff or fail to follow correct procedures, install incorrect power supply in the system, leading to severe damage to main circuit boards.	Detailed specifications in contract. Supplier experience in similar contracts. Built-in safety features of the system.	Contract to require additional power supply installation tests and checks.	$75 000	Before risk treatment, 1 in 1000. After risk treatment, 1 in 10 000.

24.11 The results of the example risk assessment, as shown in **Table 5** above, will be used as the basis for estimating supplier liability and setting appropriate supplier liability limits. The process of generating liability estimates is discussed in more detail in paragraph 27.

25. Conduct of the risk assessment

Overview

25.1 The specific nature of the proposed procurement will influence:

(a) how the risk assessment will be undertaken;

(b) the scale of the risk assessment; and

(c) to what level of detail the risk assessment will go.

25.2 While the actual form of the risk assessment will be determined by the procurement officer based on the particular circumstances of the procurement (noting that the standard promotes flexibility and tailoring of the approach to the risk assessment), this section provides some guidance on how to make that determination.

25.3 Depending on the nature of the proposed procurement, the risk assessment process can be short and straightforward or very detailed and comprehensive. The procurement officer undertaking the assessment must consider whether the procurement is a low, medium or high risk ICT procurement (see paragraph 3.5), and decide whether the agency has the internal capability and capacity to conduct an appropriate risk assessment or requires external specialist support.

Cost benefit decision

25.4 Procurement officers should bear in mind that the scale of the risk assessment undertaken must be sufficient to enable the agency to:

(a) understand where the risks lie and identify risk treatment options;

(b) understand how the risks may affect the parties' liability; and

(c) appropriately allocate liability and include risk treatment options in the contract.

25.5 Generally, the risk assessment for a low risk ICT procurement will be straightforward, and there is likely to be little benefit in spending a large amount of resources on the risk assessment process. The costs of engaging expert assistance in conducting the risk assessment should be weighed against the benefits.

25.6 On the other hand, medium and high risk ICT procurements are more likely to:

(a) require a detailed risk assessment that justifies the commitment of significant resources; and

(b) involve all relevant stakeholders and subject matter experts in the risk assessment.

26. Risks specific to each supplier

26.1 One element of a risk assessment involves an assessment of the risks associated with using a particular supplier. There are a number of criteria that might be relevant in an assessment of the supplier, including their:

(a) level of experience of doing work of the kind specified;

(b) technical capability;

(c) capacity and resources available;

(d) financial viability; and

(e) proposed contractor/subcontractor arrangements.

26.2 The risk profile of a supplier will depend on a number of factors, and it should not be assumed that a SME inherently presents greater risks than a larger supplier. A SME will often represent a low risk option - for example if they have good credentials and a sound record in doing the work specified in the contract. Large companies and corporations also may represent a low risk, as they can bring substantial resources and capacity to support complex assignments.

26.3 Each supplier should be assessed according to their relative merits, taking into account the particular circumstances of the procurement.

Information and Communications Technology Multi-Use List (ICT MUL)

26.4 The ICT MUL is a list of ICT suppliers that Australian Government agencies can use to source ICT goods and services. Agencies are not required to use the ICT MUL for their procurements, and inclusion on the ICT MUL does not imply that the Australian Government endorses the use of that supplier's product or services.

26.5 An assessment of the risks of the procurement should be conducted for all potential suppliers, including those suppliers on the ICT MUL.

26.6 More information on the ICT MUL can be found at www.tenders.gov.au/ictmul.

27. Estimating liability

Overview

27.1 The first step in estimating and allocating liability under the contract is the completion of a risk assessment, as described earlier.

27.2 A risk assessment for the purpose of estimating and allocating liability should involve:

(a) an assessment of the potential consequence of an event if that event were to occur, including the financial consequences (expressed as a dollar amount);

(b) an assessment of the likelihood that the event will occur, using an appropriate likelihood scale (see example likelihood ratings at **Appendix 6**) where the likelihood is expressed in either words (such as 'likely' or 'rare'), or as a numerical probability (such as a one in a hundred or one in a thousand).

27.3 In making the initial assessment, it is important to keep the assessments of 'consequence' separate from the assessment of 'likelihood'. For example, in assessing the potential consequence of an event you should assume that the event will occur, even if the likelihood of that event occurring is considered to be very unlikely. It is only after the 'likelihood' and 'consequence' of a risk event have been estimated that the two are brought together, usually by applying a risk priority matrix, to determine how the risk event is to be treated (see the example risk priority matrix at **Appendix 6**).

27.4 From these risk assessments, estimates of liability can be developed and, ultimately, estimates and allocations of each party's liability can be established. There are a number of ways of generating liability estimates, from very simple methods to more sophisticated modelling and simulation.

27.5 The starting point for estimating liability is to compile a list of all liability risks (a 'risk register') that describes:

(a) the risks;

(b) existing controls;

(c) the consequence of each risk;

(d) the likelihood of each risk occurring; and

(e) any additional recommended risk treatments.

27.6 Maintaining the risk register is an ongoing process, and the register should be developed throughout the risk identification, analysis and evaluation steps described earlier (refer to **Appendix 8 — Example risk register**). Once the risk assessment has been completed, the risk register should include all liability risks, their consequences and likelihood of occurring. This register is the starting point for estimating liability, and ultimately deciding on an appropriate limit to that liability.

28. Methods for estimating liability

28.1 When estimating an appropriate limit of liability, it is important to consider the risk that goods to be delivered may not be fit for purpose and/or do not meet the required specifications. Where such goods are likely to be of little or no value to the agency and will need to be replaced, it may be appropriate to ensure that the supplier is liable for at least the full cost of replacing those supplies.

28.2 It is common for agencies to employ a risk priority matrix when undertaking a risk assessment. For example, and using the example risk priority matrix at **Appendix 6**, an agency may have a requirement that a risk that is identified as 'Extreme' (e.g. assessed as 'almost certain' to occur and to result in a 'severe' consequence) must be reported to the agency's senior executive. At the other end of the matrix, agencies might decide to exclude from the calculation of the liability cap risk events that are identified as 'Low' (e.g. assessed as having a 'rare' likelihood of occurring with an 'insignificant' consequence if it did occur).

Basic liability estimate

28.3 There will be occasions when a very simple approach to estimating liability is appropriate and reasonable. The most basic method of establishing a limit of supplier liability is to use the risk register to find the risk with the highest value of consequence (expressed in monetary terms), and use this as the maximum amount for which the supplier is to be liable under the contract.

28.4 This method is used if it is improbable that more than one of the identified risks will occur through the term of the contract. The highest value risk would therefore represent a reasonable upper limit of supplier liability.

28.5 If more than one risk is likely to eventuate during the term of contract, this basic method may not be the best solution. The alternative is to adopt either the 'intermediate' or 'sophisticated' methods detailed below.

Intermediate liability estimate

28.6 Another relatively simple method of estimating liability is to add together some or all of the consequence values to form an aggregated estimate of liability. The limitation of this approach is there is only a very remote possibility that all identified risks will occur during the term of the contract or that all the damage that may be caused will amount to the summed total of the value of all the risks. Hence, this is a simplistic estimate of liability from an agency perspective and results in a liability estimate that is highly unlikely to be exceeded in the duration of the contract.

28.7 While this approach can establish a worst case estimate of liability from which a more realistic limit may be negotiated or established through discussions between the parties, it is not recommended that an appropriate level of liability be determined solely on the basis of an aggregated estimate of all liability risks. This is a reasonable approach to establishing a starting position from which an acceptable liability limit may be negotiated.

Sophisticated estimate

28.8 The most sophisticated and accurate, but also the most resource intensive, method of estimating liability is to construct a model that combines the financial impact of the consequences with the probability of the risk occurring (i.e. the likelihood).

28.9 Due to the resources required to develop, run and refine the model, and the analysis that must follow the modelling, this method is recommended only for complex procurements or for high value procurements with significant or inter-related risks and liabilities.

28.10 Due to the complexity of a sophisticated assessment, and the level of experience and expertise required to conduct such an assessment, this guide does not instruct procurement officers on how to undertake such an assessment. Instead it explains the basics of how such a model is generated and the outputs it will provide.

28.11 To accurately model the contract risks for complex procurements with significant, inter-related risks and liabilities, it is necessary to use specialised software. Such software allows the simulation of a very large number of iterations of the procurement risks (perhaps 100 000 iterations) to replicate as many possible procurement scenarios as possible. Applications with "monte carlo" simulation functions or other similar capabilities are available that will perform this simulation task. However, experience shows that it is the quality of information loaded to a simulation model, and the structure of that model, that has the greatest impact on the quality of the resultant liability estimate.

28.12 The starting point for this approach is the fully populated risk register. There is one major difference, however, in the way in which the financial consequences are estimated and recorded in the risk register. Instead of recording the worst plausible financial outcome, a three point estimate of the impact should be determined, using best case, worst case and most likely scenarios.

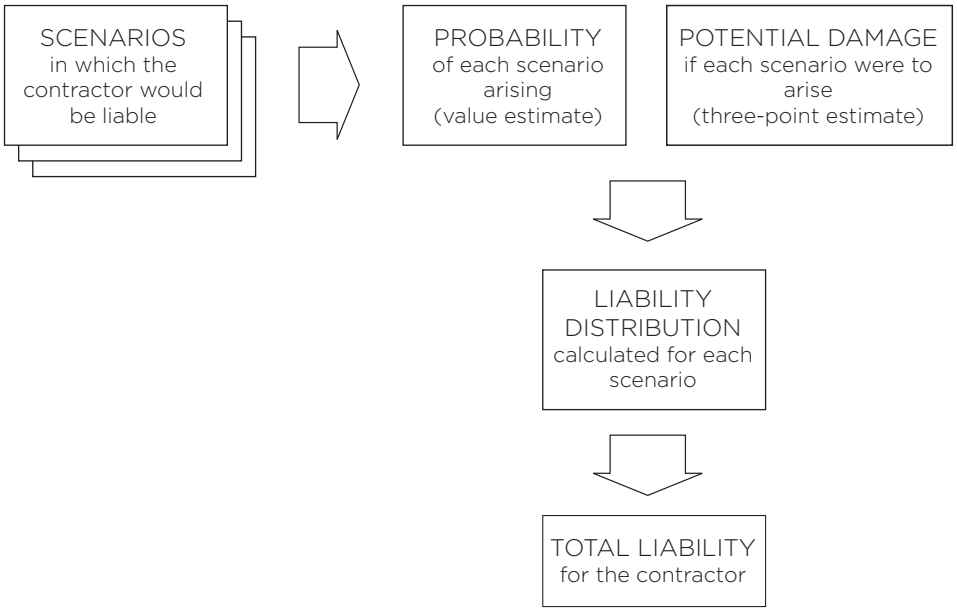
28.13 **Table 6** shows how the risk register might be amended to allow for a sophisticated approach to the liability estimate.

Table 6: Example of 'sophisticated' modelling approach

Risk number	Risk description	Controls	Additional risk treatment	Financial consequence (best case; most likely; worst case)	Likelihood
1	Supplier may use inexperienced staff of fail to follow correct procedures, install incorrect power supply in the system, leading to severe damage to main circuit boards.	Detailed specifications in contract. Supplier experience in similar contracts. Built-in safety features of the system.	Contract to require additional power supply installation tests and checks.	Best case = $1000 Most likely = $10 000 Worst case = $75 000	Before risk treatment, 1 in 1000. Following risk treatment, 1 in 10 000.

28.14 A simulation captures data that shows, over a great number of iterations, how risks might occur and their inter-relationships, based on their probability and impact. While the raw output from this simulation is a great deal of data, the model should also be able to summarise the data output in graphical and statistical formats that meet the demands of the agency. This output is used to determine a level of confidence in any range of liability limits for the proposed contract. **Figure 2** illustrates the general process.

Figure 2: Process for developing a liability model



28.15 The objective of the model is to establish, to a reasonable level of confidence, the limit of supplier liability that would be sufficient to provide the agency with liability coverage in the majority of liability events. By simulating many thousands of possible scenarios, the model will provide data to meet this objective.

PROTECTING THE AGENCY'S ABILITY TO RECOVER FROM A SUPPLIER

29. Common methods of protecting the ability to recover

29.1 Managing risk is more than merely conducting a risk assessment and including appropriate liability provisions in a contract. Liability allocated to a supplier only provides an agency with the ability to recover damages from the supplier if the supplier has the financial resources or the backing of another party (such as a parent company or insurance) to pay the damages.

29.2 There are a number of ways an agency can maximise its ability to recover damages for claims. The most common ways are listed below, and in many cases, a combination will be used. The agency may seek to:

(a) ensure that the supplier has sufficient current insurance to pay all claimable damages under the contract;

(b) ensure that the supplier has the financial capacity to self-insure for those risks, taking into account its other potential liabilities, and is able to meet from its own resources all damages under the contract; and

(c) obtain a performance security (e.g an unconditional financial undertaking) for an amount that meets (or partly meets) potential damages under the contract, and/or a performance guarantee from an entity that has sufficient resources to meet the supplier's obligations under the contract, including to be liable for damages arising under the contract.

30. Insurance – its purpose and limitations

30.1 As indicated above, the purpose of requiring a supplier to hold insurance is to reduce the risk that the supplier will not have sufficient financial resources to meet its liabilities in relation to the contract.

30.2 It is essential that procurement officers understand the limitations of insurance and do not assume that damages caused by a supplier above a liability cap will be covered by either the supplier's or the agency's insurance. As a general rule:

(a) the supplier's insurance will not cover liability above the cap (this is because the supplier is normally only insured for its liability, and the supplier is not liable for damage or loss above the cap); and

(b) most categories of liability that are likely to be capped may not be covered by insurances issued by Comcover (e.g. Comcover does not usually insure agencies for damages arising from a supplier's professional negligence or a supplier's breach of contract).

31. Insurances held by the supplier

31.1 A key issue for procurement officers is to determine what insurances the supplier should be required to hold under the contract. To do this, the procurement officer should:

(a) review the contract or project performance risks identified in the risk assessment;

(b) consider which of the risks can be insured, noting that not all risks are insurable (for example, the risk of a simple non-performance of the contract by the supplier cannot be insured against);

(c) for those risks that can be insured, determine:

(i) which party would be liable if the risk eventuated, and which party should insure against the risk;

(ii) what type of insurance is required;

(iii) whether insurance is the preferred treatment for the risk, noting that a decision not to insure may be justified if the risk is very remote (e.g. risk of confiscation in Australia) or the consequences of the risk eventuating are so catastrophic that the cost of insurance is too high (e.g. possibly environmental impairment cover); and

(iv) understand the cost to the supplier of taking out the specific insurance and how any of those costs may cause increases in the proposed contract price.

31.2 The SourceIT model contracts require a supplier to hold insurance that covers:

(a) public liability;

(b) professional indemnity;

(c) product liability; and

(d) workers' compensation as required by law.

31.2 Where an agency does not use the SourceIT model contracts, it is important to note that other ICT contract precedents (including the AGTA) do not require the supplier to hold *product liability* insurance. Agencies should consider whether they need to require the supplier to hold product liability insurance where the supplier's supply, manufacture or distribution of a product may result in liability to third parties. It is important to remember that the supplier's *public liability* policy will *not* cover these liabilities.

31.3 Procurement officers should review the risk assessment for the procurement to confirm that there are no unusual risks that may require additional or special insurance. If uncertain, the advice of an insurance expert should be sought to ensure that the *description* of the types of insurance required by the contract adequately covers the risks intended to be insured.

31.4 Where an agency requires a supplier to effect different insurances to those required under the SourceIT model contracts, it is also important to consider the availability and cost of the insurance. Requiring inappropriate insurance or insurance for risks that are remote or of low value may result in unnecessary costs to the supplier and/or the agency, and delays in finalising the contract while the required policies are put in place. Where a supplier is required to get insurance specifically for the contract, the full cost of such insurance is likely to be passed on to the agency. Further, there is no point in requiring insurance above a liability cap, taking into account per event and aggregate limits of the insurance policies, because the insurer will only pay up to the

limit of the supplier's liability. In other words, the insurance required of the supplier in the contract should be consistent with the liability provisions.

31.5 It is important to note that while the specified level of insurance should take into account the agreed level of liability of the supplier, this does not mean that the agreed level of liability should be determined by taking into account the suppliers' current levels of insurance cover. Agencies should avoid capping the supplier's liability at whatever amount may be recovered from the supplier's insurance, as discussed at paragraph 17.5.

32. Insurance held by the agency

32.1 Procurement officers should also be aware of the insurance policy coverage provided by Comcover. Procurement officers should read the full terms of the policy (the current policy is available at www.finance.gov.au). In general terms, the 2009/10 policy includes the following insurances which cover damages that an agency may suffer, or liabilities an agency may incur in relation to an ICT procurement:

(a) General liability and professional indemnity insurance covers, among other things:

(i) an agency's liability to pay compensation for bodily injury, death, sickness, disease, disability, shock, fright, mental anguish, mental injury or emotional distress;

(ii) an agency's liability arising from infringement of copyright, title or slogan, "passing off"[22] or breach of IP rights (including moral rights);

(iii) an agency's liability arising from breach of confidence, invasion of privacy or other similar misuse of information;

(iv) an agency's liability for property that is damaged, lost or which cannot be used;

(v) claims for loss caused by the execution or breach of an agency's duty that arises from the agency's operations or business.

(b) Property loss, destruction or damage insurance covers loss, destruction or damage to the agency's property;

(c) Business interruption and consequential loss insurance covers costs of interruptions to the agencies operations arising from damage, loss, or destruction of property, or an inability to access property; and

(d) Personal effects insurance covers loss, destruction or damage to the personal effects of an employee of an agency in the workplace, or while on approved travel within that person's home country.

32.2 Comcover does not automatically cover contractually assumed risks. This means that where an agency indemnifies, releases or caps a supplier's potential liability, that agency may be uninsured with respect to the contractually assumed risk (that is, uninsured for liability above the agreed liability cap unless) Comcover agrees to an extension of cover.

32.3 There is no requirement to obtain Comcover approval for liability caps (where the agency will be effectively self insuring losses from its own budget). Where the liability cap relates to an insurable risk and the agency wishes Comcover to fund potential

22 "Passing off" is a common law action used to prevent, for example business A from misrepresenting that A's goods or services are related to business B – usually where business B has valuable goodwill or reputation. An common example is where a business A sells a similar product to business B, using similar packaging and labelling (even where the names of the products are different and are clearly displayed). The law of passing off is similar to the law of misleading and deceptive conduct, and passing off actions are often brought in conjunction with an action for breach of the misleading and deceptive conduct provision of the trade practices legislation.

losses arising in excess of the cap. This approval must be sought in advance and provided in writing.

32.4 To request an extension of cover (indemnity request) from Comcover, agencies need to provide their Comcover Member Services account manager with:

(a) a copy of the relevant contract clauses relating to insurance, indemnities, liability caps;

(b) a copy of either an internal or external legal review;

(c) evidence of determination to proceed with the contract, this may be either a signed copy of the FMA Reg 10 Authorisation Form or a Minute requesting the same, or a statement that acknowledges the intent of the authorised delegate to sign the contract in its current form (eg for CAC agencies, a statement that acknowledges the intent of the authorised delegate to sign the contract in its current form is required)[23]; and

(d) a risk assessment that focuses on the credible worst case loss exposure for the insurable loss event risk/event.

33. Supplier self-insurance

33.1 It may be possible for a supplier to *self-insure* where it is in a sufficiently strong financial position to be able to meet all claimable (or certain types of claimable) damages under the contract from its own resources (this may include providing an unconditional financial undertaking instead of insurance), taking into account the supplier's total potential liabilities, including to other customers and creditors. Where the supplier is able to self-insure, the agency might obtain a lower price (e.g. where the supplier does not have to take on additional insurance and pass on the costs of that insurance to the agency).

33.2 The decision to allow a supplier to *self-insure* should only be made if the agency has undertaken a proper financial analysis of the supplier's financial position and that analysis supports the conclusion that the supplier is able to meet potential damages claims. If a decision is made to allow self-insurance, legal advice will be required to amend the standard insurance provisions in the contract.

33.3 While supplier self-insurance is occasionally accepted on high value procurements, it is usual in such circumstances to require the supplier to also provide an unconditional financial undertaking or performance guarantee for at least part of the estimated potential claimable damages.

34. Performance Securities

34.1 A performance security is an instrument that is used to reduce the risk of non-performance. There are a number of types of performance security, including:

(a) financial securities, such as financial undertakings or bank guarantees, where the security provided is a promise to pay money; and

(b) performance bonds or performance guarantees, where the security provided is a promise to ensure delivery of the goods/services, and which may also include payment of money.

34.2 Performance securities are often sought:

(a) where the incentives in the contract are not considered sufficient to drive performance by the supplier;

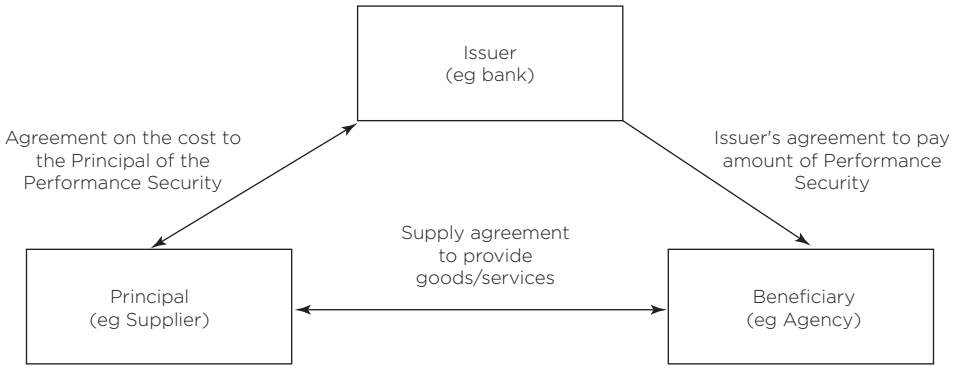
23 Note: FMA agencies will be required to provide the signed FMA Reg 10 authorisation in the event of a claim.

(b) where there are doubts as to the financial capacity of the supplier to perform the contract; and/or

(c) for large and complex projects where there are heightened risks to the agency flowing from poor or non-performance.

34.2 **Figure 3** to **Figure 6** below set out an example of a simple performance security arrangement – in this case a bank guarantee/financial undertaking arrangement.

Figure 3 - Simple performance security arrangement



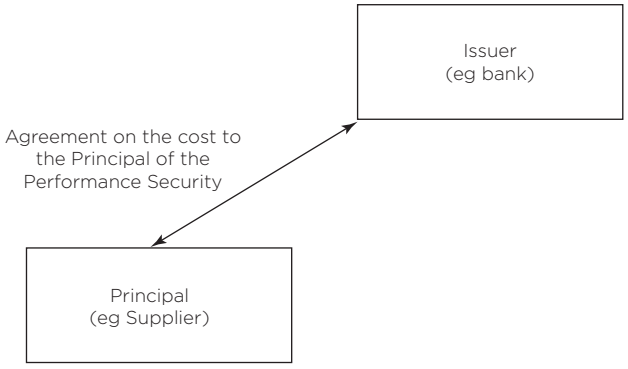
Generally these simple performance security arrangements will involve 3 agreements, 2 of which will involve the agency. Each of the 3 agreements are described briefly below.

(1) The 'Supply' contract between the agency (i.e. 'Beneficiary') and the supplier (i.e. 'Principal') to provide the goods/ services. The bank is not a party to this agreement;

Figure 4 - Simple performance security arrangement – "Supply" contract

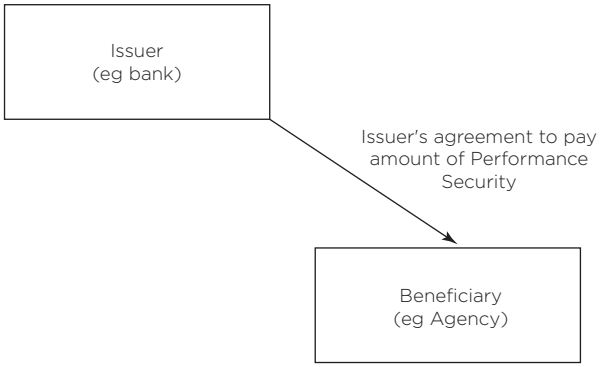
(2) The agreement between the supplier and the bank (i.e. 'Issuer') as to the terms (usually cost to the supplier) under which the bank agrees to provide the security. The agency is not a party to this agreement.

Figure 5 - Simple performance security arrangement - agreement between supplier and bank



(3) The agreement between the bank and the agency where the bank promises the agency that it will pay to the agency, on request from the agency, money up to the agreed sum of the performance security. This agreement will usually be in the form of a deed. The supplier is not a party to this agreement.

Figure 6 - Simple performance security arrangement – the performance security agreement



34.3 A key feature of performance securities is that they have few if any conditions attached (e.g. sometimes they are referred to as 'unconditional' undertakings). An unconditional undertaking means that the document will not generally be qualified by reference to the terms of the 'Supply' contract between the agency and the supplier. For example, under the arrangements described above, the bank is obliged to pay the amount of the security to the agency without the agency being required to demonstrate that the supplier is in default of its obligations to the agency under the 'Supply' contract.

34.4 The key difference between a financial security and a performance security is that a performance security is provided to ensure the goods/services are delivered, rather than payment of money (though payment of money may also be involved). It will generally be provided by a parent or related company and will involve a promise by that parent/related company to deliver the goods/services if the supplier fails to deliver.

34.5 Although financial securities may be also given by a parent company, they are typically given by independent financial institutions and, when given by a financial institution will have a cost attributable to the issue of the instrument. A risk assessment of financial and performance security arrangements should be undertaken before a performance security is sought in order to determine an appropriate sum to be payable under the security, and whether requiring a performance security is the most efficient and effective use of public money.

34.6 It is important to remember that a performance security should be securely stored and details recorded including any amounts drawn against it. FMA Order 5.1 provides that any official who receives 'bonds, debentures or other securities' must keep a register of securities and ensure their protective custody.

MANAGING RISK FOLLOWING CONTRACT EXECUTION

35. Contract management

35.1 No matter how complete the contract is in addressing each identified risk and applying appropriate liability caps, the contract will not be an effective risk management tool unless is it is well managed to ensure that each party (including the agency) meets their obligations under the contract to the standard and within the timeframes stipulated in the contract. An important element of good contract management is implementing a process of regular review to keep the risk register up to date and to manage the risks.

35.2 For guidance on contract management, agencies should refer to relevant Australian Government guidance (e.g. *Contract Management: Better Practice Guide* available at www.anao.gov.au).

APPENDIX 1 — GLOSSARY

AGTA	Australian Government Telecommunications Arrangements
CAC Act	*Commonwealth Authorities and Companies Act 1997*
CAC Regulations	*Commonwealth Authorities and Companies Regulations 1997*
Consequence	An outcome of an event expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
CPGs	*Commonwealth Procurement Guidelines 2008* (Financial Management Guidance No.1)
FMA Act	*Financial Management and Accountability Act 1997*
FMA Regulations	*Financial Management and Accountability Regulations 1997*
GITC4	Version 4.1 of the Australian Government GITC framework standard legal documentation is available at www.gitc.finance.gov.au). GITC is a set of legal documents used by the Australian Government to create contracts for the purchase of IT goods and services. Version 4.1 includes updates designed to address impacts of policy and program changes and offer consistency with SourceIT model contracts where possible. According to the GITC website, it is possible that GITC4.1 will be replaced by 'SourceIT' branded ICT contract solutions in the form of model contracts, clauses or other support mechanisms/tools.
ICT	Information and communications technology
ICT liability circular	Finance Circular 2006/03 *Limited Liability in Information and Communications Technology Contracts* issued on 15 August 2006 outlines the ICT liability policy.
ICT liability policy	The Australian Government's policy that requires agencies subject to the FMA Act to, in most cases, cap the liability of ICT suppliers at appropriate levels. Unlimited liability should only be required when there is a compelling reason.
IP	Intellectual property
IT	Information technology
Likelihood	A qualitative description of probability or frequency.
RFT	Request for tender
RFQ	Request for quote
Risk assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk analysis	The systematic process to understand the nature of, and to deduce the level of, risk.
Risk criteria	The terms of reference against which the significance of a risk is evaluated.
Risk evaluation	The process of comparing the level of risk against given risk criteria to assist in decisions about risk treatment.
Risk identification	The process of determining what, where, when, why and how something could happen.
SME	Small to medium enterprise

APPENDIX 2 – FINANCE CIRCULAR 2006/03

Australian Government

Department of Finance and Administration

Finance Circular 2006/03

To all agencies under the *Financial Management and Accountability Act 1997* (FMA Act agencies)

Limited Liability in Information and Communications Technology Contracts

Purpose

This Circular articulates and provides guidance on the Australian Government's policy on the capping of liability when entering into Information and Communications Technology [1] (ICT) contracts.

Target Audience

This Circular applies to all agencies subject to the *Financial Management and Accountability Act 1997* (FMA Act).

The Policy

1. Australian Government policy is that the liability of ICT suppliers contracting with agencies should, in most cases, be capped at appropriate levels. Unlimited liability clauses should only be required when there is a compelling reason.

2. The policy governing limited liability for ICT contracts is to be an Australian Government policy for the purposes of Regulation 9 of the *Financial Management and Accountability Regulations 1997* (FMA regulations) and the *Commonwealth Procurement Guidelines* (CPGs).

Context

3. For the purpose of this policy, a liability cap on supplier's liability is defined as an arrangement whereby a supplier's liability for damage or loss incurred by the Commonwealth is limited to a certain amount. A liability cap only applies to the parties to the contract and does not include:
   - limiting the supplier's liability to compensate a third party; or
   - compensating the supplier for damage suffered directly by the supplier.

[1] Information and Communications Technology is a term that encompasses the use of hardware, software and services to create, store, retrieve, transfer, process and present information.

4. The Australian Government has a general principle in regard to risk management that risks should be borne by the party best placed to manage them - that is, the Commonwealth should generally not accept risks which another party is better placed to manage.

5. Unlimited liability should not be requested for ICT procurement contracts unless it is an accurate reflection of the potential risks.

6. The Government's policy on capping liability in ICT contracts, as detailed in this Circular, creates greater certainty for ICT suppliers and for agencies. The policy also promotes efficiencies for suppliers when developing their tenders and efficiencies for both agencies and suppliers in the contract negotiation process.

7. It is important that officials continue to obtain appropriate advice, including risk management and legal advice, in relation to the liability clauses to be included in ICT contracts.

Background

8. The CPGs sets out the Australian Government's policy on procurement, reflecting its overarching policy on risk management:
   - risks should be borne by the party best placed to manage them;
   - if there is a compelling reason to limit a supplier's liability, any indemnity, liability cap or similar arrangement should be of limited scope and with specified maximum liabilities;
   - as part of considering such a limit, FMA Act agencies should refer to the requirements set out in Finance Circular 2003/02 and the accompanying *Guidelines for Issuing and Managing Indemnities, Warranties, Guarantees and Letters of Comfort.* These Guidelines provide definitions of indemnities, warranties, guarantees and letters of comfort, information on how they may be used, and considerations regarding the application of FMA Regulations 9 and 10. Care should be taken when drafting clauses to ensure an arrangement is a liability cap as opposed to an indemnity arrangement. Regardless of whether the clause is called a liability cap, indemnity, release or by any other name, it is the effect of the clause that must be taken into account;
   - for each proposal to limit a supplier's liability to the Australian Government a risk management process must be undertaken, including undertaking a risk assessment and obtaining legal advice where appropriate, having regard to the complexity of the purchase and the level of risk; and
   - the potential costs of any liability cap must be considered when assessing value for money.

Applying the Policy

9. Officials should refer to their agency's Chief Executive's Instructions for information on risk assessment and procurement procedures.

10. The following provides a step-by-step approach that agencies can follow when applying the policy of capping liability in ICT contracts.

Step 1 – Determine the appropriate liability regime for your ICT project.

- With a default starting position of applying a liability cap, a formal risk assessment assists in establishing whether the size, complexity or inherent risk of the project are such that the agency should reconsider whether a liability cap should be offered.

Step 2 – Determine the appropriate level for the initial estimate of the liability cap.

- Whenever an agency is considering capping a supplier's liability for an insurable risk, the agency should contact Comcover to determine whether its own insurance cover is affected. It is a condition of Comcover's agency coverage that it have the rights of the agency to recover a loss – this is known as subrogation.
- In the event of a claim by an agency for a loss arising from an event for which a supplier has legal liability, but is protected by a liability cap, Comcover's subrogation rights may be prejudiced. Where this occurs, Comcover may limit its coverage of the agency to the amount that Comcover may recover from the supplier. The agency would then be required to bear any loss above the cap.
- Contact with Comcover should initially be pursued through an agency's Chief Finance Officer area or Risk Management Area.

Step 3 – Determine how the liability issues will be handled in the procurement process and contract.

- Agencies can consider using either of the following approaches when going to the market:
  - identify the liabilities to be capped within the request documents and state the proposed level of the liability cap, allowing (if desired) tenderers to propose an alternative level (or range of levels) of liability cap in their submissions and adjust pricing accordingly; or
  - inform potential suppliers that due to the nature of the procurement a cap will not be applied, but only in circumstances where the size, complexity or inherent risk of the procurement require that a liability cap not be offered.

Step 4 – Establish agreement and complete the contract.

11. It is particularly appropriate for agencies to consider negotiating liability caps in ICT contracts in relation to the following matters:
    - standard breach of contract in relation to service delivery obligations; and
    - supplier liability arising from negligent acts or omissions, (other than negligence related to personal injury and property damage and other than losses that result from a breach of intellectual property rights, confidentiality, privacy and security obligations or unlawful conduct as explained below).

12. Unless there is a compelling reason otherwise, it is generally appropriate for agencies to retain unlimited liability clauses in ICT contracts in relation to the following matters:
    - personal injury including sickness or death - it is preferable that agencies require unlimited liability rather than placing a value (liability cap) on personal injury or death caused by a supplier;

- unlawful or illegal acts - suppliers should not have their liability limited in relation to unlawful acts or illegal activity;
- damage to tangible property - standard contract practice includes unlimited liability with respect to property damage and it would be unusual to treat ICT contracts differently;
- intellectual property obligations - liability for intellectual property infringement in respect of ICT products supplied by a supplier is a fundamental consideration in such contracts as ownership and title of intellectual property rights need to be properly protected;
- confidentiality and privacy obligations - limiting liability in ICT contracts may interfere with the proper implementation of principles, protocols, practices and legislative obligations with respect to confidentiality and privacy; and
- security obligations - it would not be prudent to dilute or affect the Australian Government's position with respect to security matters by capping the liability of suppliers in procurement.

Record Keeping

13. Agencies' decisions when approving a spending proposal, including whether to have unlimited liability, must be properly documented.

Additional Resources

14. Readers should also be aware of these additional resources which may have a bearing on the capping of a supplier's liability:
    - Department of Communications, Information Technology and the Arts (DCITA), *A Guide to Limiting Supplier Liability in Information and Communications Technology (ICT) Contracts with Australian Government Agencies*.
    - *Commonwealth Procurement Guidelines*.
    - Finance Circular 2003/02 *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort.*

Contacts

15. Questions with regard to this Circular should be directed to the Procurement Agency Advice Branch at procurementagencyadvice@finance.gov.au or visit Finance's website at http://www.finance.gov.au (under the Government Finances menu).

16. Questions regarding the DCITA publication *A Guide to Limiting Supplier Liability in Information and Communications Technology (ICT) Contracts with Australian Government Agencies* should be directed to DCITA's ICT Development Branch at cappingliability@dcita.gov.au.

John Grant
Division Manager
Procurement Division
Asset Management Group
15 August 2006

APPENDIX 3 – PROCUREMENT PROCESS TIMELINE

A common question in the course of undertaking procurement is 'when is the best time to conduct the assessment of liability?' As discussed in this guide, the assessment of liability is closely related to the conduct of a risk assessment and, in most cases, these assessments take place concurrently.

1. Draft request for tender (RFT)

1.1 Procurement officers should conduct a preliminary assessment of risk and liability before, or at the same time as, the tender documentation (RFT or request for expression of interest etc) is being drafted. This allows procurement officers to have treatment strategies developed in response to the assessment of risks addressed in contract provisions and conditions of the tender. Using the early risk assessments, the procurement officer can start to build up a picture of the liability risks, their likelihood of occurrence and their general value. This value can be communicated to industry as an estimate of liability limits in the draft contract included in the RFT.

2. Source selection and contract negotiation

2.1 Once a preferred tenderer is selected and contract negotiations begin, the procurement officer will have a better idea of the risks to the procurement, based on the supplier's proposed approach, track record and commercial details. General estimates of liability developed earlier are now updated on the basis of more accurate information and can be introduced into negotiations with the preferred tenderer for discussion and agreement.

3. Contract performance

3.1 Risks in procurements change over time and as other factors change. Therefore, procurement officers should plan to conduct periodic assessments of risk and liability, especially for large contracts that span a number of years. Appropriate milestones within the procurement may be selected to conduct the assessments, such as six monthly performance reviews, major delivery milestones, technical reviews or other suitable activities. It is never too late to identify risks and to develop strategies for their treatment. There is also great value in conducting these assessments with the participation and support of the supplier.

4. Contract Disengagement

4.1 The process of contract disengagement may involve transition to a new service provider, re-engagement of the current service provider, or simply contract closure and finalisation of any outstanding services. Legal, financial, logistical, administrative and physical matters will all need to be finalised in accordance with contract provisions as part of the disengagement process.

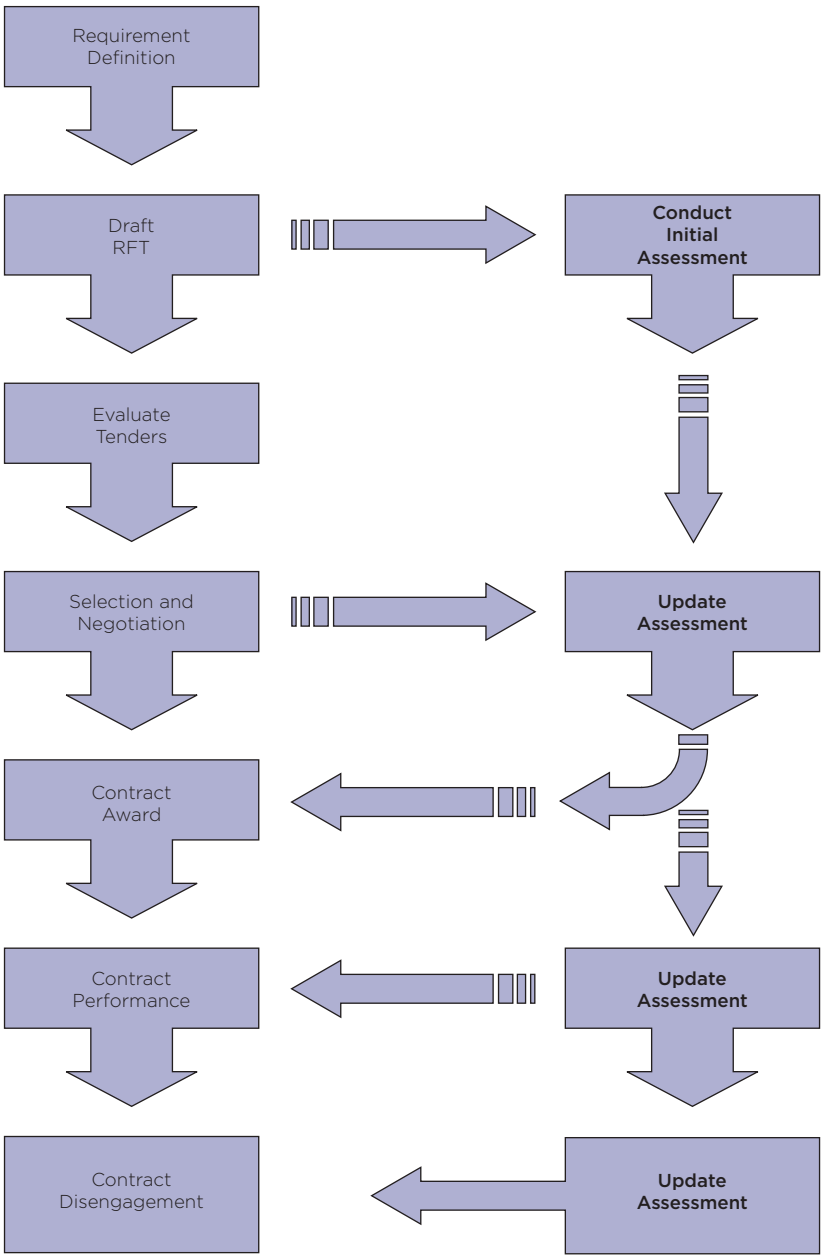
4.2 Procurement officers will need to identify the risks to successful contract disengagement and develop appropriate treatments for those disengagement risks assessed as being unacceptable in their current state. Procurement officers may wish

to draw upon lessons learnt from other contract disengagements, Transition-Out Plans and Project Closure Reports that are an excellent source of information on what might go wrong during contract disengagement.

4.3 A detailed risk assessment should be undertaken prior to commencing detailed disengagement planning activities. Results of the disengagement risk assessment, particularly any recommended treatments, should be included in contract disengagement plans, and monitored and reviewed in accordance with normal risk management practices.

4.4 **Figure 7** illustrates the recommended risk assessment points against a generic procurement timeframe. Procurement officers should not be constrained by this example and are encouraged to plan for a risk assessment program that best suits their requirements and the nature of the procurement activity.

Figure 7: Contract and risk assessment schedule



APPENDIX 4 – CASE STUDIES

This appendix considers five case studies to illustrate how the practices described in this guide could be applied to various ICT procurement situations.

1. Case study 1

Purchase of flat screen monitors to replace conventional computer monitors

1.1 Background

An agency had a requirement to replace all conventional computer monitors with flat screen equivalents. The procurement had two components: (1) supply and (2) installation. The total cost of supplying the monitors was estimated to be more than $80 000, and so the agency issued an RFT asking potential suppliers to quote to supply the monitors. As the installation of the monitors was estimated to cost less than $80 000, an RFT was not issued for the installation work, and a work order was instead directed to the agency's existing ICT support services provider panel for this work.

Supply contract

1.2 Preliminary risk assessment and preparation of RFT

The procurement officer undertook a preliminary and high level risk assessment of procurement risks at the same time as the RFT was being drafted (the risk assessment did not identify the full range of possible damages, as key details of the procurement would be unknown until the tenderers' solutions were evaluated). However, the procurement officer's initial risk assessment concluded that the procurement was a simple procurement and low risk.

The RFT included a contract based on the model SourceIT hardware contract which includes liability clauses consistent with the ICT liability policy. The RFT stated that respondents were to indicate compliance or otherwise with the clauses and specify a proposed liability cap.

1.3 Evaluation of tenders

The preferred tenderer demonstrated an innovative technology flat screen at a total cost of $2 million, which was substantially cheaper than the next lowest tendered price. The evaluation committee assessed the innovative flat screen as demonstrating improvements in performance, although the technology had not yet been trialled in significant numbers by any organisation. The preferred tenderer agreed in substance to the liability clauses and offered a liability cap of $2.3 million.

1.4 Conduct of further risk assessment to address specifics of tenders

As part of the tender evaluation phase, a further risk assessment of the tendered solutions was undertaken. The innovative flat screen was considered to carry some additional risks compared to mature and well tested flat screen products. The risk assessment identified a number of risks specific to the innovative technology flat screen including:

(a) possible delays in production and delivery of the large quantity of screens required by the agency;

(b) possible poor reliability and screen failures well before the anticipated end of life; and

(c) a shortage of spares and support equipment after installation (until the supplier built up its support capability).

The assessment found that the probability of delays and/or premature screen failures was moderate, given the new technology used and the lack of historical data on the reliability of the new screens. The cost to the agency of these risks occurring was high. However, the benefits of the innovative screen were still considered to outweigh the risks and the innovative screen was selected as the preferred solution.

1.5 Assessment of liability cap

Despite the initial impression that the procurement was a simple low risk procurement, the tender evaluation resulted in a preferred solution which introduced new and more significant risks. The procurement officer therefore conducted another more comprehensive risk assessment with agency stakeholders and technical experts in the lead up to contract negotiations, to identify risk treatment strategies and to assess whether a liability cap of $2.3 million was sufficient.

The more comprehensive risk assessment concluded that while the agency could reasonably cope with delays in delivery of the new monitors with little or no financial impact, premature screen failures and a lack of appropriate support for such failures would have a significant financial impact. In the worst case, the agency would be required to obtain alternative supplies of screens in very short timeframes, and probably at higher costs. The cost of such a worst case scenario was estimated in the assessment as being $2.2 million. Other risks were costed at considerably lower values.

The agency therefore, agreed to the supplier's proposed liability cap of $2.3 million. The agency also required the supplier to agree to the inclusion of specific requirements in the contract such as a detailed acceptance testing regime, warranties in relation to meeting delivery timeframes, liquidated damages, minimum reliability performance and mandated levels of spares holdings and support capability.

Before entering into the contract, the procurement officer reviewed the supplier's insurance policies to confirm compliance with the insurance requirements in the contract.

Installation contract

1.6 A high level risk assessment (involving the completion of a risk register incorporating the conclusions reached at a brainstorming session attended by key stakeholders) was performed in relation to the flat screen installation work. The risk register recorded the view that the most extreme consequence of a risk eventuating was $90 000 in damage to the agency and that the likelihood of this occurring was one in a hundred. The likelihood of more than one risk eventuating and the combined damages exceeding $90 000 was assessed as unlikely. Three quotes were sought from panel members. The preferred quote offered to provide the services for $85 000, with supplier liability capped at the value of the installation contract. In contract negotiations, the supplier agreed to an increase in the liability cap to $90 000, the agency agreed to cap economic loss arising from the supplier's negligent act or omission, and the supplier agreed to unlimited liability for damage caused to the agency's tangible property (including the screens).

2 Case study 2

Installation of a network with normal business applications in a new agency facility

2.1 Background

An agency was building a new facility and, before moving in, needed to install a computer network, including all infrastructure, file servers, switching, workstations and basic applications. The agency sought to appoint a single supplier to be responsible for the installation work, as well as for provision of network support for the first three years after installation. The procurement had to go to tender as it was above $80 000 (estimated in the range of $750 000), and the agency issued an RFT requesting potential suppliers to quote to provide the services.

2.2 Preliminary risk assessment and preparation of RFT

The procurement officer prepared a context statement (similar to the example shown in **Table 3**, paragraph 20.4) to help identify key project objectives, stakeholders and evaluation criteria. The procurement officer's initial view was that the procurement was not a complex procurement and was medium risk.

The procurement officer undertook a preliminary risk assessment of the procurement at the same time as the RFT was being drafted. The officer conducted the risk assessment by assembling a group of stakeholders that included facilities, systems, and user group representatives. The group completed a risk register (similar to the register shown in Table 4, paragraph 22.13) by considering each key aspect of the scope of work. The procurement officer used the consequence scales and likelihood ratings in **Appendix 6 – Qualitative measures of consequence and likelihood** to qualitatively assess the risks.

As this was a new facility (and hence would not be occupied until completed), and in view of contemporary building standards and ICT requirements, the risk assessment found that only a few risks associated with the scope of work carried moderate to severe consequences.

The incorrect installation of the network was assessed as resulting in a major consequence if not detected before occupation of the facility. However, taking into account the technical specifications of the site (which required only a basic, non-complex network to be installed) and the acceptance testing regime (which required the network to be fully tested prior to occupation of the facility), stakeholders considered the likelihood of incorrect installation affecting the ongoing operation of the facility – i.e. after it was occupied – to be rare. However, the stakeholders also concluded that there was a moderate likelihood that at least part of the network might fail the initial acceptance tests, leading to a delay in the occupation of the facility while the problem was rectified. The financial impact on the agency if it was unable to occupy the facility on the required date would be significant, and was assessed as a major consequence.

The stakeholders also identified risks associated with a single supplier conducting the full scope of work, which included a variety of different services ranging from design and installation of the physical ICT infrastructure of the facility, to delivery of a network service to end users.

Stakeholders therefore concluded that the supplier was likely to subcontract a significant amount of the work. The risk of poor subcontractor arrangements impacting adversely on the project was identified as likely to occur given the agency's knowledge of the limited number of suppliers capable of performing the entire scope of work. The consequence of the risk eventuating was the same as for the delay caused by a failure to meet acceptance testing (as above).

A further risk identified by stakeholders was the risk of poor through-life support for the network due to multiple and complicated subcontractor arrangements. However, stakeholders considered that this risk could be treated through the head contract with the principal supplier, and the requirement that the agency approve all subcontractor arrangements. This risk was assessed as having a moderate likelihood of occurring, but due to the basic level of support to be provided and the technical specifications, was assessed as only being of minor consequence.

2.3 Limit of liability

The procurement officer and stakeholders estimated that the occupancy date for the agency could slip by as much as 30 days while initial network problems were resolved, and this would result in additional rental costs of up to up to $100 000. While there would also be considerable inconvenience associated with such delay, these would not result in losses that the agency was legally entitled to claim from the supplier. Further, while poor through-life network support would reduce the agency's efficiency while the problems were being resolved, such losses would be difficult to quantify and recover from the supplier.

While the likely costs of the delays were estimated to be $100 000, as the computer network would be of little or no value to the agency if it was completely unfit for purpose, the liability cap also included the full cost of replacing the network, estimated at $610 000. The procurement officer included liability clauses consistent with the ICT liability policy and a limit of liability of $710 000 ($610 000 + $100 000 for delays) in the RFT and draft contract, which was still less than the estimated full contract value of $750 000 (which included $140 000 for network support). Additionally, the evaluation criteria in the RFT and the supplier obligations in the draft contract were drafted to emphasise the importance of the supplier's management of subcontractors. The RFT stated that respondents were to indicate compliance or otherwise with the clauses and specify any cost implications to the agency of alternative liability caps.

The agency contract manager undertook six monthly performance reviews of the network support services to monitor ongoing service delivery.

3. Case study 3

Installation of a project management software application on an agency's network

3.1 Background

An agency required a new project management software application to be installed on its network. The required application was a proven, mature application, known to work well with other applications on the network. The licences for the application were purchased under a whole-of-government software agreement. The agency sought a supplier to install the application. The agency estimated that the cost of installation would be $60 000. The agency sought quotes from suppliers on its existing IT services provider panel.

3.2 Preliminary risk assessment and preparation of request for quote

The procurement officer prepared a context statement (similar to the statement shown in **Table 3**, paragraph 20.4) to help identify key project objectives, stakeholders and evaluation criteria. The procurement officer's initial view was that the procurement would be simple and low risk.

Before releasing the RFQ, the procurement officer conducted a risk assessment of the procurement. The assessment was completed in several hours through a brief brainstorming session with agency network and application specialists. This approach was taken as the procurement was considered simple and low risk. The main risk identified in the brainstorming session related to loss or corruption of data due to negligent installation.

Given the decision to select a mature and well-proven application, the assessment concluded that the likelihood of negligent installation was low. The likelihood of significant data loss or corruption was also considered to be low, as the agency intended to backup all data before installation. The brainstorming session estimated that recovering data from backup tapes and fixing poor installation could cost the agency $10 000. The agency sought a liability cap of the value of the contract. The procurement officer noted that the value of any data lost or corrupted would be excluded from the liability limit and be treated as an unlimited liability.

Nonetheless, the procurement officer decided that the consequence of the risk eventuating was significant enough to include provisions in the contract that required the supplier to perform specific acceptance tests and ensure data recovery processes were in place prior to implementation of the new application.

Before entering into the contract, the procurement officer reviewed the supplier's insurance policies to confirm compliance with the insurance requirements in the contract.

4. Case study 4

Development and rollout of an agency website portal capable of a range of e-business and government business functions

4.1 Background

As part of an agency's new approach to providing more online services, it decided to implement a new website, including a portal to provide a range of services online to its customers, including some basic e-business functions. The agency sought a supplier or suppliers to design, implement and maintain the new portal.

4.2 Preliminary risk assessment and preparation of RFT

The procurement officer prepared a context statement (similar to the statement shown in **Table 3**, paragraph 20.4) to help identify key project objectives, stakeholders and evaluation criteria. In the course of collecting and analysing information to complete the context statement, the procurement officer formed the view that:

- the cost of procurement is likely to be in the range of $850 000 to $900 000;
- the procurement is most likely a borderline simple/complex procurement and medium risk; and
- the agency should issue an RFT requesting suppliers to quote to supply the full services (with the intention that one prime contractor will be responsible for the full service provision).

The procurement officer undertook a preliminary risk assessment of the procurement at the same time as the RFT was being drafted. The officer conducted the risk assessment by assembling a group of stakeholders that included the ultimate agency 'project owner', some agency IT officers and user group representatives. The group completed a risk register (similar to the register shown in **Table 4**, paragraph 22.13) The procurement officer had initially assessed the procurement to be a medium risk activity, largely influenced by the few online and e-business services that had

initially been identified for inclusion in a basic website. However, as drafting of the RFT progressed, the agency 'project owner' recognised the opportunity presented by the portal and requested the procurement officer to expand the scope of work to increase the number of online services to be covered by the portal, with some time and business critical functions to be included. The complexity of the required design services significantly increased.

The procurement officer and the group of stakeholders appointed to undertake the risk assessment came to the view that the change in scope made it difficult to fully understand the risks and estimate an appropriate liability cap. A specialist consultant was engaged to facilitate and conduct a workshop and to perform the analysis of the results.

The workshop identified a significant number of risks that related to the integrity of the proposed portal, including the following.

1. Failure or lack of availability of the portal could lead to agency customers being unable to access or provide information in the legislated timeframes.
2. Sensitive business or personal information provided by agency customers through the portal could be lost or inadvertently passed to other agencies or organisations.
3. Inaccurate information from the portal could cause the agency to mislead its customers.
4. Agency customers could lose revenue or business opportunities through failures of the portal.

The assessment found that the financial impact to the agency could be considerable if the risks were to occur—well in excess of the value of the contract which was quite moderate by comparison. Based on experiences elsewhere within the government, risks such as those identified by the stakeholders were considered to have a reasonable likelihood of occurring.

The specialist consultant worked in close association with the procurement officer to develop a model of the risks, their financial impact and probability of occurrence. This model was based on outputs from the workshop. A number of simulations were run to estimate the range of possible outcomes of the risks, and these simulations were run over many thousands of iterations with specialised software to support the analysis. Sensitivity analysis was undertaken to ensure the model was robust and that no one particular risk was skewing the analysis or driving the model.

The procurement officer sought a level of confidence in the analysis, so that the agency could be informed that there was a high degree of certainty as to the worst case liability levels the agency could face. The model and analysis indicated (with a 99.99 per cent level of confidence) that agency liability for failures in the portal would not exceed $5 million in total. As a result, the procurement officer stipulated a proposed limit of supplier liability of $5 million in the RFT and draft contract.

The RFT included a contract with liability clauses consistent with the ICT liability policy. The RFT stated that respondents were to indicate compliance or otherwise with the clauses, including a liability cap of $5 million, and to specify any cost implications to the agency of alternative liability caps (including the cost benefits of a lower cap or caps).

4.3 Evaluation of tenders

The preferred tenderer offered to provide the services as a prime contractor for $1.5 million, with a liability cap of $5 million in accordance with the liability clauses set out in the RFT.

Further, provisions were included in the draft contract to cover specific requirements (availability and accessibility of the portal to agency customers, sensitivity and accuracy of data, contingency planning, data recovery, and business continuity requirements).

Before entering into the contract, the procurement officer reviewed the supplier's insurance policies to confirm compliance with the insurance requirements in the contract.

4.4 Ongoing project management

The agency project owner continued to update the risk register throughout the project to ensure that identified risks were properly managed.

5. Case study 5

Development and implementation of a new, complex operational system

5.1 Background

An agency had a requirement to develop a management system to integrate a range of systems and technologies into a single source of information and knowledge for use in highly critical, operational activities. The information that needed to be integrated varied in complexity and maturity, in the hardware used, and came from a number of sources, within and outside the agency.

5.2 Preliminary risk assessment and preparation of RFT

The procurement officer undertook a preliminary risk assessment of the procurement at the same time as the RFT was being drafted. The officer conducted the risk assessment by conducting several in-depth brainstorming sessions with a group of stakeholders that included the ultimate agency 'project owner' and a number of agency IT officers with different types of IT expertise. The group completed a risk register (similar to the register shown in Table 4, paragraph 22.13) by considering each key aspect of the scope of work.

The key conclusion reached was that the task of defining the information sources and integration tasks would be particularly difficult, due to the range and age of the sources and functions. The key stakeholder group was of the view that the development of the new system would cost approximately $2.5 million. Following the brainstorming session, the procurement officer decided that the procurement was sufficiently complex to require the expertise of a risk assessment specialist to facilitate a further risk assessment workshop and to analyse the results before the RFT was completed.

5.3 Further risk assessment

The workshop participants concluded that there were a range of products on the market that were very effective in integrating a variety of information sources. It was considered that off the shelf products would help reduce the risk somewhat, if they were used. The impact on the agency of the new system failing was considered significant, but hard to quantify. However, most risks identified related to those systems from which information would be obtained and the agency's ability to access existing software and code in order to make the integration work. There were also some risks relating to licensing of existing software to facilitate the integration, and meeting specific agency operational requirements which would mean that even off the shelf software would require some modification. Some of these risks appear below.

1. Software and code may not be available for some of the older systems that need to be integrated.

2. Companies might be reluctant to grant a licence to access or modify the code of existing systems to enable integration to occur, or might charge excessive fees for the licence.
3. Development of new software or modification of existing off the shelf software to meet agency requirements could delay delivery of the system and/or increase costs.
4. Changing agency requirements on the functions and outputs of the new system could lead to delays and cost increases.
5. Failure of the system during critical operations could lead to the agency suffering significant losses.

Input from stakeholders during the workshop confirmed the procurement officer's view that access to the workings of the older systems would be difficult and time consuming, so the probability of this risk occurring was very high. Likewise, the stakeholders were able to confirm that there was a strong possibility that licences to obtain and modify existing software would be difficult to obtain and would impede the contract if they were not obtained. However, the probability that the new system would fail in operation was assessed as reasonably low.

5.4 Limit of liability

The risk assessment concluded that the direct cost to the agency in terms of operational failure resulting from system failure was not significant in financial terms, although system failure would impact on national interests. The consequential loss that the government could 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) was assessed as being in the range of $20 million.

A number of models were developed and simulated by the consultant, addressing a range of possible risk scenarios and impacts. These were run through many thousands of iterations to give the agency an idea of the range of possible outcomes. The models were able to demonstrate with a 99.99 per cent degree of confidence that the agency could face financial impacts of up to $25 million as a result of the stated risks occurring.

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. Additions to the draft contract also included specific requirements on guaranteeing access to software, code and licences at reasonable and fully costed rates, and guaranteed availability and reliability levels of the system in operation. System backup and business continuity plans were also mandated in the contract.

As the proposed liability cap was greatly in excess of the contract value ($2.5 million), all of the suppliers responded to the RFT identifying the level of liability as an issue for further negotiation and indicating a degree of non-compliance with the liability clauses in the draft contract. The liability cap was also identified as an assumption affecting the tendered prices. During negotiation with the preferred supplier, the supplier set out the commercial consequences of carrying such a high level of liability in its accounts, and the increased costs that would be passed on to the agency if the supplier had to carry that level of liability. The supplier also provided details of its risk management processes and treatment strategies to reduce both the likelihood and consequence of some of the identified risks. Taking into account this additional information and additional treatment actions that the agency would also introduce, the agency assessed that these reduced the risk of the agency suffering losses from the procurement. The agency negotiated a reduction in price in return for reducing the liability cap to $10 million. While this was still significantly higher than the contract value, it was a level of risk that the supplier was commercially able to accept and that the agency considered to be an appropriate allocation of risk.

APPENDIX 5 – USEFUL REFERENCES

1. Key legislative provisions

The main legislative provisions affecting procurement in Australian Government agencies (principally Australian Government departments, but also prescribed Commonwealth agencies) are the:

- *Financial Management and Accountability Act 1997* (especially sections 5 and 44);
- *Financial Management and Accountability Regulations 1997* (especially regulations 3, 7, 8, 9, 10, 12 and 13); and
- the Chief Executive's Instructions for each agency, issued under FMA Regulation 6, in accordance with section 52 of the FMA Act.
- The main legislative provisions affecting procurement in other relevant Australian Government bodies (Commonwealth authorities and wholly owned Commonwealth companies) are the:
- *Commonwealth Authorities and Companies Act 1997* (especially sections 47 and 49);
- *Commonwealth Authorities and Companies Act Regulations 1997* (especially regulation 9);
- *Finance Minister's (CAC Act Procurement) Directions 2004*; and
- *Financial Management and Accountability (Finance Minister to Chief Executives) Delegation 2009*.

2. Key policies relevant to ICT procurement

Finance Circular 2006/03 *Limited Liability in Information and Communications Technology Contracts* issued on 15 August 2006 outlines the Australian Government's ICT liability policy.

The Financial Management Guidance series of publications includes:

- No. 1 Commonwealth Procurement Guidelines, December 2008
- No. 2 Australian Government Foreign Exchange Risk Management Guidelines, September 2006.
- No. 3 Guidance on Confidentiality in Procurement, July 2007.
- No. 6 Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort, September 2003 and accompanying Finance Circular 2003/02.
- No. 8 Guidance on the Listing of Contract Details on the Internet (Meeting the Senate Order on Department and Agency Contracts), January 2004No. 9 Australian Government Competitive Neutrality Guidelines for Managers, February 2004.
- No. 10 Guidance on Complying with Policies of the Commonwealth in Procurement January 2010.
- No. 13 Guidance on the Mandatory Procurement Procedures, January 2005.
- No. 14 Guidance on Ethics and Probity in Government Procurement, January 2005
- No. 15 Guidance on Procurement Publishing Obligations, July 2007

- No. 20 Guidance on the Gateway Review Process - A Project Assurance Methodology for the Australian Government, August 2006

3. Other relevant policies and guidance include:

- Standards Association of Australia, Australian and New Zealand Standard, *AS/NZS ISO 31000:2009 Risk management - Principles and guidelines, 2009*. Australian National Audit Office, Contract Management: *Better Practice Guide - Developing and Managing Contracts,* available at www.anao.gov.au.
- Comcover Better Practice Guide – Risk Management, June 2008 available at www.finance.gov.au/comcover/better-practice-guide.html.
- Australian National Audit Office, *Selecting Suppliers – Managing the Risk* available at www.anao.gov.au.
- Department of Finance and Deregulation, Finance Circular 2003/02 *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort* available at www.finance.gov.au/publications.
- Department of Finance and Deregulation, Finance Circular 2009/05 *Commitments to spend public money (FMA Regulations 7-13)* available at www.finance.gov.au/publications.
- Department of Finance and Deregulation, Finance Circular 2007/01 *FMA Regulation 10* available at *www.finance.*gov.au/publications.
- Management Advisory Board, MAB/MIAC Report No. 22 *Guidelines for Managing Risk in the Australian Public Service*, October 1996. Availability details are available at www.apsc.gov.au.
- Dale F Cooper, Stephen Grey, Geoffrey Raymond and Phil Walker (2004): *Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements*, John Wiley & Sons, Chichester, ISBN 0-470-02281-7

4. Websites

Standards Australia — www.standards.org.au.

ICT Multi Use List — www.tenders.gov.au.

Commonwealth Procurement Guidelines —

www.finance.gov.au/publications.

APPENDIX 6 – QUALITATIVE MEASURES OF CONSEQUENCE AND LIKELIHOOD

1. Consequence scales

Rating	Description
Severe	Would cause huge financial loss.
Major	Would cause major financial loss.
Moderate	Would have a moderate effect causing high financial loss.
Minor	Would have a minor effect causing medium financial loss.
Insignificant	Would have an insignificant or low effect causing low financial loss.

2. Likelihood ratings

Likelihood	Description
Almost certain	Expected to occur in most circumstances
Likely	Will probably occur in most circumstances
Possible	Could occur at some time
Unlikely	Not expected to occur
Rare	Will occur in exceptional circumstances only

3. Risk priority matrix

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Medium	Medium	High	High	Extreme
Likely	Medium	Medium	Medium	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

APPENDIX 7 – CHECKLIST OF TYPICAL ICT RISKS

Procurement officers should be wary of relying too heavily on an existing checklist of risks rather than developing, in conjunction with stakeholders, a list that is tailored to the specific procurement.

Notwithstanding the above, checklists can help procurement officers understand common risks that may impact upon their type of procurement and provide a starting point for creating a list tailored to their project and resultant contract.

1. Example checklist of ICT contract risks

1.1 Agency risks

Technical risks

- ☐ Poor information is provided by the agency during the tendering process, leading to inaccuracies in tenders and the contract.
- ☐ The agency does not provide material and information as contracted, leading to the supplier being unable to provide services in the required timeframe.
- ☐ Information provided by the agency is inaccurate or unrealistic, leading to delays in the supplier delivering the contracted services.
- ☐ The agency is unable to provide sufficient resources to manage the contract and supplier interface.
- ☐ The contract statement of work is poorly written and does not accurately reflect the actual services to be provided or customer requirements.
- ☐ Existing agency systems are not properly maintained which leads to delays in the delivery of services by the supplier.
- ☐ There is poor systems 'housekeeping' by the agency, including unauthorised software and hardware installations, and poor asset management, resulting in the supplier being unable to effectively undertake the contracted services.
- ☐ Activities associated with other ICT projects and day-to-day operations clash with priority supplier tasks, leading to schedule delays.
- ☐ Undocumented configuration changes in agency ICT systems could result in additional work by the supplier.
- ☐ The agency's test environment is not adequate for supplier tests.
- ☐ The agency's security and facility access regulations could cause the supplier difficulties in undertaking the contracted services.
- ☐ Agency organisational changes cause supplier difficulties and result in change to contract requirements.
- ☐ Problem resolution between multiple agencies could cause difficulties for the supplier in delivering contracted services.
- ☐ Elements of the ICT infrastructure are under the control of third parties and influence the ability of the supplier to provide contracted services.
- ☐ The supplier might be unable to access third party software used by the agency on the system, leading to delays and frustration of the contract.

Commercial risks

- ☐ The agency fails to adopt the new services or systems.
- ☐ Lack of communication within the agency about the supplier's activities and contract responsibilities could delay the supplier in undertaking the contracted services.
- ☐ The agency's workforce does not fully cooperate with the supplier in the delivery of the services leading to delays.
- ☐ The agency lacks expert advice and guidance, leading to difficulties in the supplier delivering the services required.
- ☐ The agency's corporate knowledge and key skills are lost or minimised as a result of the supplier undertaking the work.
- ☐ The agency's business requirements change after the contract is signed and lead to difficulties with the supplier.
- ☐ A lack of controls leads to undisciplined or unauthorised changes to contract scope or services.

1.2 Supplier risks

Technical risks

- ☐ Complexity brought about by multiple systems interfaces cause service delivery failures.
- ☐ Supplier integration of services with existing ICT systems or communications networks is difficult and causes delays or termination of the contract.
- ☐ The supplier does not use proven and current technology in the provision of its services.
- ☐ The supplier does not allow for continuous improvement resulting in inability to meet contracted service levels.
- ☐ The supplier is unable to improve its workforce skill levels through the life of the contract, leading to failure to achieve contracted service levels.
- ☐ Mobility of agency workforce affects the ability of the supplier to complete the contracted work.
- ☐ Poor reliability of new systems leads to failure to meet contracted service levels.
- ☐ The supplier is unable to maintain the necessary skill levels over the course of the contract, leading to a reduction in service levels.
- ☐ Staff turnover and loss of skills within the supplier workforce leads to poor levels of service as the contract progresses.
- ☐ The supplier is unable to provide the infrastructure support or assets it promised in the contract, leading to delays and possible termination of the contract.
- ☐ The supplier is unable to access the technology required to undertake the contracted services.
- ☐ The supplier cannot obtain the necessary security clearances to provide the services required by the contract.
- ☐ The services provided by the supplier are unable to meet the growth and flexibility requirements of the agency.
- ☐ The supplier is unable to provide services as per the contract due to unplanned changes in the agency ICT environment.

- ☐ Failure of the supplier to obtain, or loss of, quality and other required accreditations leads to inability to complete the services as contracted.
- ☐ Poor design of software and documentation by supplier leads to difficulties in through-life support.
- ☐ The supplier conducts unauthorised activities in agency ICT systems, leading to system problems, damage or failures.
- ☐ The supplier uses inappropriate tools to deliver the services leading to poor service or physical damage to agency systems.
- ☐ The supplier introduces unauthorised software or technology to the agency system.
- ☐ Proper processes and procedures are not followed by the supplier in introducing new systems or technology, leading to installation of incompatible or unsuitable items leading to a breach of contract conditions.
- ☐ The supplier moves or removes agency equipment or material, leading to loss of agency assets.
- ☐ The supplier reduces the level of diligence in the care of agency material on the assumption that the agency will meet replacement or repair costs for lost or damaged material.
- ☐ Sensitive information on agency networks is accessed by the supplier, leading to breaches of confidentiality and privacy.
- ☐ The supplier misuses agency data for its own purposes.
- ☐ The supplier does not recognise the priority to be afforded to critical services (medical, financial, security) leading to agency dissatisfaction, and possible termination of contract.
- ☐ The supplier refuses to release proprietary information or technical data to the agency as required under the contract, leading to an inability of the agency to support the system into the future.
- ☐ The supplier causes unacceptable disruptions to agency operations in the conduct of its work.
- ☐ The supplier does not have a disaster recovery plan for serious virus infections, meaning on discovery of a virus infection, the supplier could not take immediate action to eradicate the virus, restore operational efficiency or recover lost data.
- ☐ The supplier's products or systems introduce bugs or viruses into the agency network.
- ☐ The supplier does not provide all information and assistance necessary to conduct disengagement as efficiently and effectively as possible.

Commercial risks

- ☐ The supplier is unable to recruit suitable staff to provide the services required under the contract.
- ☐ The supplier disrupts agency services by actively seeking to recruit key agency personnel during the early stages of the contract.
- ☐ The supplier is not adequately resourced to manage the workloads required by the contract.
- ☐ Services are delayed or impacted by inappropriate or under-resourced supplier transition activities.

- ☐ Poor subcontractor management or subcontractor performance leads to inability of the supplier to meet contract requirements.
- ☐ The supplier or one or more of its subcontractors has a legal arrangement with an entity that creates a conflict or perceived conflict of interest with the performance of the contract.
- ☐ The supplier does not comply with occupational health and safety laws, or related agency obligations and policies.
- ☐ The supplier becomes insolvent, or ceases or threatens to cease to carry out its business, and makes an arrangement with or for the benefit of its creditors that could make the continuance of the contract unworkable.

1.3 Joint risks

- ☐ The agency and supplier experience a cultural clash leading to misunderstandings, disputes and a poor relationship.
- ☐ Criteria for acceptance of supplier services are not well understood or agreed prior to the acceptance activity, leading to disputes over the acceptance activity.
- ☐ The agency and supplier disagree over the measurement of service level performance during the course of the contract.
- ☐ Lack of agency and supplier disaster recovery and business continuity plans results in major loss of services in the event of a system failure.
- ☐ The supplier's expectations of services and support do not align with the agency's requirements for continuous operations, leading to contract disputes.
- ☐ Inadequate agency performance benchmarks and reporting tools, or failure of the supplier to maintain adequate documentation or appropriate tools to manage the contract, could lead to ineffective performance measurement.

APPENDIX 8 – EXAMPLE RISK REGISTER

Risk number	Risk description	Controls	Consequence	Likelihood	Additional risk treatment	Responsible officer
1	Supplier may use inexperienced staff who fail to follow correct procedures and install incorrect components in the agency system, leading to severe damage to the agency system.	Detailed technical specifications in contract. Supplier experience in performing similar contracts. Built-in safety features of the system.	$75 000	1 in 1000	Contract to include additional installation acceptance testing and check requirements.	Engineering Manager
2	Supplier subcontractors may be late in delivering materials and services, leading to delays in meeting installation deadlines and additional costs of running old systems.	Selection of well-proven subcontractors. Detailed agreements with subcontractors. Effective subcontractor management processes.	$25 000	1 in 100	Include requirement that agency approve selection of subcontractors.	Contracts Manager
3	Delivered systems prove to be unreliable, leading to failure to achieve required service levels.	Selection of off-the-shelf technology. Selection of contractor with experience in this kind of work.	$45 000	1 in 100	Include additional incentives and service credits in contract for system reliability.	Contracts Manager
4	Failure by the supplier to obtain obligatory certification or accreditation results in frustration of the contract.	Selection of a contractor with prior experience.	$350 000	1 in 10 000	Add provisions to the contract that allow termination if certification or accreditation not achieved in reasonable timeframe.	Contracts Manager
5	Supplier is unable to secure the required financial guarantees, insurances and other mechanisms.	Tender evaluation process.	$350 000	1 in 1000	Add provisions to the contract that allow termination by agency if financial protections not in place shortly after contract execution. Ensure required financial guarantees and certificates of insurance have been received before work commences.	Contracts Manager
6	Poor design of software and documentation leads to delays and poor system performance in implementation and through-life support.	Selection of off the shelf technology. Selection of contractor with experience in this kind of work.	$50 000	1 in 100	Include provisions for system development reviews, and document reviews in the contract.	Engineering Manager

Risk number	Risk description	Controls	Consequence	Likelihood	Additional risk treatment	Responsible officer
7	The supplier is unable to maintain workforce skill levels through the life of the contract, leading to failure to achieve contracted service levels.	Tender evaluation process. Selection of contractor with experience in this kind of work.	$45 000	1 in 100	Require an endorsed human resources plan as a contract deliverable. Review service level requirements that may be impacted by workforce problems.	Contracts Manager
8	The integration of new systems with existing software could cause the network to crash or the loss of critical data.	Selection of off-the-shelf technology. Selection of contractor with experience in this kind of work. Supplier knowledge of legacy systems.	$500 000	1 in 1000	Require extensive lab test and trials of new systems before acceptance and installation. Improve data backup capabilities before installation of new system.	Engineering Manager
9	Supplier staff could conduct unauthorised activities in agency ICT systems, leading to system problems, damage or failures.	Tender evaluation process – select contractor with experience in this kind of work. Undertake security checks of key supplier personnel.	$75 000	1 in 1000	Require endorsed procedures and security manuals as a contract deliverable. Review service level requirements that may be impacted by inappropriate access.	Contracts Manager
10	Criteria for acceptance of supplier services may not be well understood or agreed prior to the acceptance activity, leading to disputes over the acceptance activity and delays in commencing services.	Acceptance criteria well defined in the draft contract.	$25 000	1 in 10 000	Review acceptance processes with the supplier prior signing the contract.	Contracts Manager
11	Agency and supplier disagree over the measurement of service level performance during the course of the contract, which may lead to poor performance of services.	Proven and well defined service level requirements in draft contract and reporting mechanisms.	$45 000	1 in 100	Review service level definitions and reporting requirements with the supplier before signing the contract. Do not impose unrealistic service levels.	Contracts Manager
12	The supplier may be unable to access third party software used by the client on the system, leading to delays and frustration of the contract.	Tender evaluation process – ensure agency has right to sub licence agency software to the supplier or select supplier with right to use other software.	$350 000	1 in 1000	Add provisions to the contract that allow termination if access to third party software cannot be achieved in a reasonable timeframe.	Contracts Manager

APPENDIX 9 – CONTRACTUAL RISK MANAGEMENT MECHANISMS

Forms of Protection		Definition	How this Protects an Agency
PERFORMANCE SECURITY	**Unconditional Financial Undertaking (UFU)**	An Unconditional Financial Undertaking (UFU) is a financial instrument that allows the holder of the instrument to access money on demand. (To simplify, it can be thought of like a bank cheque). For example, an Agency may ask the supplier to arrange for a bank to provide a UFU to the Agency (eg $5m). The UFU is a direct promise from the bank to the Agency that the bank will pay that amount on demand. As the UFU is unconditional, the Agency may ask the bank to pay the Agency an amount up to the limit of the UFU (eg $5m), and the bank must pay the Agency that amount (eg $5m). The Agency will not have to prove to the bank that the supplier is in breach, etc. However, the Contract between the Agency and the supplier sets out the conditions under which the Agency will have a right to call on the UFU. The Agency will be in breach of the Contract if it accesses the money contrary to the Contract. *(eg – in simple terms, the arrangement involves:* ■ *a promise from the bank to the Agency to pay the amount of the UFU on request from the Agency;* ■ *a promise from the Agency to the supplier under the Contract to only ask for the UFU in accordance with the Contract; and* ■ *a promise from the supplier to repay the bank if a call is made on the funds.)*	The UFU provides an Agency with the ability to immediately access funds to compensate for losses suffered by the Agency and caused by the supplier under the Contract.
	Performance Guarantee	A Performance Guarantees is usually used where the supplier is an entity (eg a subsidiary) put forward by a parent company to enter into the Contract. If the supplier fails to perform, the recipient of the Performance Guarantee (eg an Agency) can require the guarantor (ie the parent company) to step in and perform the Contract.	An Agency can require the guarantor to perform the Services / assume the liabilities of the supplier under the Contract.
INSURANCE	**Public Liability Insurance**	Public liability insurance covers the insured's legal liability to the public for bodily injury or damage to tangible property. Does not usually cover pure economic loss.	This insures the supplier for any damage it may cause to an Agency's property, including property entrusted to the supplier by the Agency.
	Product Liability Insurance	Product liability insurance covers losses arising out of the defective nature of goods supplied / installed by the insured.	This insures the supplier for any damage it may cause to an Agency (including intangible damage / damage to computer software) as a result of defective delivery of the Services.
	Professional Liability Insurance	Covers the insured's liability to third parties for breach of a professional duty of care owed in contract or at general law. Usually does not cover tangible property damage or personal injury.	This insures the supplier against professional errors or omissions that may cause damage to an Agency, including in relation to trade practices liability and infringement of a third party's intellectual property rights.
	Workers Compensation / Employers liability Insurance	This is compulsory insurance for all employers, covering the statutory liability to workers suffering an injury or disease arising in the course of employment. In this circumstance it is also required to cover common law liability.	Ensures that the supplier can meet claims by workers injured while performing the Services.
	Specific Insurance	Usually effected in respect of a specific item of property to provide cover in respect of accidental loss or damage resulting from certain events. May also apply to other identified risks.	An Agency may request a supplier specific insurance policy to protect against specifically identified risks.

Limit of Protection offered	Cost of Protection	
Limited to the amount of the UFU (eg $5m). The Agency and the supplier will agree the amount prior to entering into the final Contract. Limited by the conditions in the Contract, including the agreed liability cap as applicable.	The supplier pays the bank a fee for providing the UFU, and would usually recover the amount of that fee from the Agency (eg as a pass-through expense). As the amount of the UFU is to always be available to meet a call on the funds by the Agency, and as the supplier is liable to repay the bank the amount of the UFU, there is a cost to the supplier in not being able to use those funds elsewhere in its business, and the supplier may also seek to pass on some of those costs to the Agency. The cost of the UFU is dependent on the amount of the guarantee, market interest rates and the credit rating of the supplier. A Recent example of cost is $60,000/pa for a $20m undertaking.	**Unconditional Financial Undertaking (UFU)**
Usually the guarantor is required to assume complete liability.	Usually at the guarantor's expense, but the guarantor, through the supplier, may seek to pass on some of those costs to the Agency.	**Performance Guarantee**
Limited by the required maximum amount of insurance agreed by the parties under the Contract. Limited by the agreed Liability Cap as applicable.	Provided at supplier's expense.	**Public Liability Insurance**
Limited by the required maximum amount of insurance agreed by the parties under the Contract. supplier Limited by the agreed Liability Cap as applicable.	Provided at supplier's expense.	**Product Liability Insurance**
Limited by the required maximum amount of insurance agreed by the parties under the Contract. Limited by the agreed Liability Cap as applicable.	Provided at supplier's expense.	**Professional Liability Insurance**
Unlimited with respect to any statutory liability. Limited by the required maximum amount of insurance agreed by the parties under the Contract in relation to common law liability.	Provided at supplier's expense.	Workers Compensation / Employers liability Insurance
Limited by the commercial availability of the requested insurance. Limited by the agreed Liability Cap as applicable.	The supplier would be expected to pass the fee on to the Agency, either included in the contract price or, as a Pass-Through Expense	Specific Insurance

NOTES

NOTES

NOTES