Australian Government

Department of Communications, Information Technology and the Arts

A guide to limiting supplier liability in ICT contracts for Australian Government agencies

Developing and implementing a risk assessment and mitigation strategy

November 2005

ISBN X XXX XXXXX X

Disclaimer

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

(a) make no representation and give no warranty as to the accuracy of the information contained in this Guide;

(b) do not accept any responsibility for any error or inaccuracy in, or omission from, this Guide (whether negligent or otherwise); and

(c) are not liable for any loss or damage arising as a result of any person acting or refraining from acting on any recommendation or on the basis of any information contained in this Guide.

Information on the Authors

Blake Dawson Waldron (BDW) has extensive experience in advising Australian Government departments and agencies, as well as State and local governments, on government outsourcing, tendering, market testing and procurement initiatives.

BDW's legal advisors have particular experience in ICT procurement and have advised on the identification of specific liability risks in high value ICT procurements, risk allocation and liability related clauses, the insurance policies available to meet those requirements, and the detailed estimation and modelling of contractor liability limits. BDW conducts legal risk assessments and assists agencies to develop sourcing strategies and assess, negotiate and manage ICT procurement arrangements.

Broadleaf Capital International (BCI) is a group of specialist consultants providing advice, facilitation and training in the areas of project risk management, strategic and organisational risk management, procurement, contract management and negotiation, risk training, quantitative risk modelling and benchmarking.

BCI has specialist risk advisors who sit on the Standards Australia Sub-Committee on risk management and who have written a number of internationally acclaimed books on the identification and management of risks in large procurements, based on their experience across a wide range of sectors and industries. BCI has more than fifty years of experience in managing risks in public sector procurement.

CONTENTS

1. Foreword

2. Introduction

2.1 The ICT Liability Policy was approved by the Minister for Finance and Administration and the Minister for Communications, Information Technology and the Arts on [insert date]. The ICT Policy requires *Financial Management and Accountability Act 1997* (FMA Act) Agencies to, in most cases, cap the liability of ICT suppliers at appropriate levels. Unlimited liability should only be required when it is justified by the size, complexity or inherent risk of a project. The ICT Liability Policy as at [insert date] is at **Appendix 2 – ICT Liability Policy**.

2.2 The ICT Liability policy has been specifically developed by the Australian Government for ICT contracts to reflect the following particular characteristics of ICT procurement:

- always insisting on unlimited supplier liability significantly reduces market competition, as many ICT suppliers (and particularly SMEs) are not prepared to accept such liability;
- always insisting on unlimited supplier liability may result in Agencies paying a higher than necessary contract price as suppliers may include the cost of excessive insurance cover and their own risk premium in their price;
- some IT development is high risk for both parties and a more alliance-based or cooperative approach to sharing risk is sometimes necessary to find a supplier willing to undertake the work; and
- it is often difficult to pinpoint the exact cause of a catastrophic IT system failure, particularly where there are more than two parties with interconnecting responsibilities.

2.3 Compliance with the ICT Liability Policy will require Agencies to apply best practice risk management to estimate an appropriate limit for an ICT supplier's liability. Adopting a more sophisticated approach to estimating appropriate limits on ICT supplier liability will be one of the essential steps in the procurement process, and will ensure that the procurement satisfies the overriding principle for Australian Government procurement of achieving value for money.

2.4 Achieving value for money includes balancing the likelihood of the risk event occurring against the cost of mitigating or insuring against that risk. Where liability rests with the supplier, the supplier will usually build the cost of meeting that liability into its price, which cost is ultimately borne by the procuring Agency. Insisting that all risks, no matter how remote, be insured against will not necessarily deliver the Agency value for money.

2.5 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 a liability regime suitable for all ICT contracts.

2.6 This Guide is particularly targeted to "non-complex" ICT procurements that:

(a) will not severely or critically affect the Agency's functions or service delivery if the supplier fails to deliver under the contract (i.e. delivery failure is not "catastrophic"); and

(b) have a low to medium contract price.

2.7 For complex or high value procurements, the Guide provides a framework for undertaking risk assessments and determining liability caps. However, in the case of such contracts, 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 caps) will need to be drafted. Agencies may also need to allocate additional resources for on-going risk management.

2.8 All ICT contracts, whether they are for the supply of basic consumables or for developmental technology, present some level of risk to the Agency and the supplier. When entering into a contract of any kind, it is important for all parties concerned to understand the nature of the risks involved, allocate the management of the risks to the most appropriate party, and take all reasonable actions to eliminate or reduce the risks to an acceptable level. This is accomplished through conducting a risk assessment. Those risks that remain once all reasonable actions are taken can then be addressed through the estimation and application of a limit on the liability of one or more parties to the Contract.

2.9 For "non-complex" contracts, the Guide describes a practice or approach for assessing risk and allocating liability that involves:

(a) identifying the risks that, if they were to eventuate, would cause damage to either the Agency or the supplier;

(b) quantifying the damage likely to be incurred for each risk that eventuates, assessing the likelihood of each risk (or a group of risks) eventuating, and calculating an acceptable liability cap;

(c) allocating liability between the parties, taking into account:

(i) Government policy in relation to leaving certain liabilities uncapped (such as personal injury or death), unless otherwise justified;

(ii) the respective abilities of each party to manage or mitigate the risks; and

(iii) the costs associated with accepting liability; and

(d) applying appropriate mechanisms to:

(i) reduce the likelihood of the identified risks occurring (eg. security checks);

(ii) mitigate the effects of risks if they eventuate (eg. insurance, back-up tapes); and

(iii) ensure that Agency exposure is appropriate.

2.10 The following table describes categories of ICT contracts to highlight the types of contracts where additional risk modelling may be required. Risk modelling and legal consideration of liability clauses would normally be required for complex procurement.

Simple Procurement	Borderline Simple/complex Complexity will ultimately depend on circumstances	Complex Procurement
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 undertake a data set standardisation project and develop a common platform for the submission of data across agencies.	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; - significantly enhance risk management assessment; and - have, as a key feature, improved security (eg. public key infrastructure and encrypted transactions).
The supplier is required to deliver desktops ordered by the Agency using its approved equipment catalogue.	The supplier is required to integrate a current, mature application into an Agency management information system.	The supplier is required to provider IT support services to approximately 20,000 accounts. Numerous interfaces exist between supplier's responsibility and Agency responsibility.
The supplier is required to undertake the rollout of a desktop refresh.	The supplier is required to develop and implement a number of network support and administration tools across a large Agency.	The supplier is required to design and implement a new and very large network across an Agency with numerous and disparate functions.

3. What goods and services are the subject of the ICT Liability Policy?

3.1 The ICT Liability Policy applies to the procurement by an Agency of any good or service subject to the Government's Endorsed Supplier Arrangement.

3.2 At the date of this Guide, the following goods and services are listed as subject to the ESA.

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

(d) **Major Office Machines (MOM)**: Printers, photocopiers, faxes, and electronic whiteboards.

4. Who must comply with the ICT Liability Policy?

4.1 The ICT Liability Policy applies to all FMA Act Agencies undertaking ICT procurement. Compliance with the Government's ICT Liability Policy is necessary to ensure that the procurement of ICT goods and services is in accordance with the *FMA Regulations*, which require the approver of a proposal to spend public money to be satisfied that the proposed expenditure is in accordance with the policies of the Commonwealth.

4.2 Bodies subject to the *Commonwealth Authorities and Companies Act 1997* (CAC Act) (CAC Act Bodies) are legally and financially separate from the Commonwealth and are not generally required to comply with the ICT Liability Policy, but are encouraged, where appropriate, to adopt ICT procurement practices that are consistent with the policy. CAC Act Bodies that are specified in the CAC Regulations for the purposes of section 47A of the CAC Act can be required to comply with the ICT Liability Policy if notified in writing by the Finance Minister. All CAC Act Bodies can be required to comply with the policy if notified by the responsible minister in accordance with section 28 of the CAC Act.

5. Application of the ICT Liability Policy in the Australian Government Procurement Framework

5.1 The ICT Liability Policy is part of the Australian Government procurement policy framework and must be applied in the context of the Government's general policies, in particular:

(a) the FMA Act and Regulations;

(b) the CPGs;

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

(d) Finance Circular No. 2004/10 Using the Financial Management and Accountability Regulation 10 Delegation.

The Australian Government's Procurement Policy Framework is described in detail at **http://www.finance.gov.au/ctc/procurement_policy_framework.html**.

5.2 Paragraphs 6.10 to 6.18 of the CPGs set out the principles that apply generally to procurement. For non-ICT procurements, the CPGs impose a general rule that supplier liability should be unlimited unless the Agency can justify capping the supplier's liability.

5.3 The ICT Liability Policy qualifies the principles in the CPGs by imposing a general rule that supplier liability for ICT procurements should be capped at appropriate levels unless the size and complexity of the procurement means that the supplier should accept unlimited liability.

5.4 Importantly, although the ICT Liability Policy qualifies the CPGs on capping supplier liability, the policy otherwise requires compliance with the CPGs. Proper implementation of the ICT Liability Policy requires Agencies to undertake a risk assessment to analyse the risks of liability arising, the impact of such risks eventuating, and the appropriate level of any cap.

5.5 Legal advice should also be obtained where appropriate, taking into account the complexity of the purchase and the level of risk.

5.6 When undertaking the risk assessment and determining the allocation of liability between the parties, Agencies should have regard to the following principles provided in the CPGs:

- the principle in paragraph 6.14 of the CPGs that where a supplier's liability is capped, each liability cap must, wherever possible, be of a limited scope and with specified maximum liabilities, both in relation to each event that can cause liability to occur and the number of those events;
- the principle in paragraph 6.16 of the CPGs that the direct or indirect costs to the Agency of agreeing to limit a supplier's liability through a liability cap must be considered by the Agency when assessing value for money; and
- the recommendation in paragraph 6.17 of the CPGs that better practice request documentation will include a draft contract with clear liability provisions, and will require potential suppliers to indicate compliance against each clause of the draft contract, including liability provisions, 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.

6. What is a Liability?

6.1 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 the supplier to pay fees in return for the supplier's proper performance of the contract;

(b) the supplier will agree to be liable to the Agency for the consequences of some events (eg. the supplier accepts liability to pay for damage to the Agency's property caused by the supplier's negligent performance of the contract); and

(c) the Agency and supplier may share liability for the consequences of some events (eg. the Agency agrees to a cap on the supplier's liability for damage caused by a supplier breach of contract in exchange for a more competitive price).

7. Capping Liabilities

Overview

7.1 Subject to the exceptions listed in **paragraphs 7.7** to **7.12 below**, the ICT Liability Policy supports capping, at appropriate levels, of the supplier's direct liability arising from:

(a) **breach of contract**; and

(b) **negligence**.

(An explanation of the meaning of "direct and indirect liability" is set out in the table identifying the different types of supplier liability and the recommended default position in relation to capping at **Appendix 3 – Table of liabilities for ICT contracts.**)

7.2 In some cases, the supplier will also seek to cap its liability for indirect losses. This request will usually involve capping the supplier's obligation (under the standard indemnity clause in most Australian Government contracts – see for example clause 22 of GITC4) to:

(a) pay for unique losses which would not ordinarily flow from the breach but which the parties were aware might arise in the particular instance (sometimes known as "consequential losses"), and

(b) reimburse the Agency for third party claims against the Agency arising out of the supplier's act or omission (known as an indemnity).

7.3 Procurement officers need to be cautious (and should seek legal advice) before agreeing to cap supplier liability for indirect losses so that the cap does not inadvertently have same the practical effect as the Agency giving an indemnity in favour of the supplier. This is because:

(a) an indemnity (as defined in the Guidelines to Finance Circular No. 2003/02) is a legally binding promise whereby a party agrees to accept the risk of loss or damage another party may suffer; and

(b) by capping the supplier's indemnity to an Agency for third party claims, the Agency is agreeing to accept the risk of loss or damage that a third party suffers (as a result of the supplier's act or omission) above that cap.

7.4 There are certain standard Commonwealth approaches (partly driven by Australian Government 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 advice before departing from any of these approaches.

7.5 Australian Government contracts generally require unlimited supplier liability in respect of the following types of damage:

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

(i) intellectual property obligations;

(ii) confidentiality obligations;

(iii) privacy obligations;

(iv) security obligations;

(b) all damage (direct and indirect) arising from an unlawful, or wilfully wrong, act or omission by or on behalf of the supplier;

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

(d) personal injury, including sickness and death.

7.6 In determining whether or not to cap supplier liability for any of the supplier activities or types of damages referred to in **paragraph 7.5**, procurement officers should have regard to the legal and policy reasons (discussed below) that underpin the tendency to require unlimited supplier liability.

7.7 Liability arising from breaches of Intellectual Property obligations

There is no legal restriction on the capping of liability for breach of intellectual property (**IP**) obligations. However, supplier liability is usually left unlimited 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 IT products supplied by a contractor is similarly fundamental and should therefore not be excluded or limited.

7.8 Liability arising from breaches of Confidentiality and Privacy obligations

There is no legal restriction in Australia on the capping of liability for breach of privacy and confidentiality obligations. However, supplier liability is usually left unlimited because of the view that:

(a) the public should have confidence that the Commonwealth will protect third party confidential information and personal information collected by or on behalf of the Commonwealth - this confidence will be undermined if the Commonwealth passes such information to contractors whose liability in relation to their obligations to protect the material is capped;

(b) the Commonwealth may be under a moral obligation to at least advise those parties whose confidential information and personal information it collects, that suppliers dealing with that information have capped liability in respect of their responsibility to protect the information; and

(c) limitations or exclusions of liability in IT 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.

7.9 Liability arising from breaches of supplier security obligations

There is no legal restriction in Australia (or instruction in the Protective Security Manual) on the capping of liability for breach of a supplier's security obligations. However, the supplier's liability is usually left unlimited 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.

7.10 Liability arising from an unlawful or wilfully wrong supplier act or omission

Common law principles restrict the ability of a party to indemnify another party for liability arising from unlawful activity. Consistent with this is the view that the supplier liability for an unlawful or wilfully wrong act or omission should be unlimited because the Government should not be seen to protect or reward unlawful acts or deliberate wrongdoing.

7.11 Personal Injury, Sickness and Death

Unlike some countries, there is no "blanket" legal restriction in Australia on the capping of liability for personal injury and death, although some legislation prevents contracting out of statutorily imposed liability in relation to certain types of personal injury and death (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).

However, supplier liability is normally left unlimited because the risk of third party claims for personal injury or death arising from supplier behaviour under ICT contracts is usually not high and, from a policy perspective, the Australian Government's preference is not to place a value (the liability cap) on personal injury or death that may arise in the performance of a contract. Furthermore, as the risk of personal injury or death being caused by suppliers under ICT contracts is usually not high, suppliers are usually able to obtain appropriate insurance (such as public liability, product liability and professional indemnity insurance) at commercially acceptable premiums.

7.12 Damage to Tangible Property

There are valid commercial reasons for Agencies requiring suppliers to accept unlimited liability in respect of property damage. (Indeed, unlimited supplier liability for property damage is normally required in both public and private sector contracts.) The main reason relates to the fact that Comcover is unlikely to provide an Agency with building and contents insurance for losses caused by a supplier that are above a liability cap because:

(a) clause 2.10.9 of the standard Comcover policy provides that Comcover is subrogated to the insured's rights of recovery in the event of a claim by the insured - that is, to the extent that the insured has rights of recovery against a third party, Comcover will pay the insured's claim and then seek to recover those amounts in the insured's name from the third party; and

(b) to the extent that an insured agrees to cap a third party's liabilities, this would limit Comcover's rights of subrogation in the event of a claim by the insured. Clause 2.9.13 of the standard Comcover policy therefore relevantly provides that Comcover will not pay for loss, destruction, damage or liability arising from any claim:

> "… if you have… compromised your legal position to the extent you have prejudiced Comcover's position."

8. The liability cap clauses

8.1 Proforma clauses which reflect the above approach to capping supplier liability are set out in **Appendix 4 - Proforma Liability Capping Clauses**. Procurement officers should seek legal advice before departing from, or negotiating changes to, the proforma clauses, GITC 4 or the Agency's own liability capping clauses.

8.2 Procurement officers seeking to negotiate changes to the liability capping clauses should have regard to the following key commercial issues:

(a) caps should ideally be per event (that is per each single occurrence or a series of related occurrences arising from a single cause);

(b) if an aggregate cap is included in the contract, it should be higher than the per event cap (eg. $2 million per event, but $4 million in the aggregate);

(c) the amount of liability cap should be reviewed each time that the contract is varied or extended;

(d) the cap should ideally operate both ways – that is it should cap the supplier's liability to the Agency and the Agency's liability to the supplier.

8.3 Separate negotiations may be required in relation to "consequential" or "indirect" losses. Suppliers may seek a total exclusion of liability for damages of this nature.

9. Other Liability Related Clauses

9.1 Capping liability is only one of a number of possible 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. For example, it is possible to draft a liability cap that, when combined with the supplier indemnity to the Agency, inadvertently has the effect that the Agency ends up indemnifying the supplier in respect of certain liabilities to third parties. It is therefore particularly important to seek legal advice if, when negotiating a liability cap, the supplier requires the Agency to amend any of the liability clauses used in the Agency's proforma contract (especially the liability cap clause and any definition of loss).

9.2 Some of the clauses that the suppliers may seek to amend include:

(a) The "**performance**" or "**delivery**" clauses that impose an obligation on the supplier to perform, and for which 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".

(b) **Warranty** clauses by which one party warrants or guarantees to 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".

(c) **Exclusion** clauses that excuse a failure by either party to achieve a guaranteed outcome in certain defined circumstances (bad weather, strikes, accidents, hold-up in input supplies, etc). These clauses are essentially in the form of

> "neither party is liable to the other party in respect of any delay or failure to perform its obligations if and to the extent such delay or failure is caused by an event of force majeure".

(d) **Indemnity** clauses which generally do not deal with failure of a supplier to perform (though they can be used for this purpose) so much as accidents/events caused by the supplier that result in personal injury, death, property damage or financial loss, including claims by third parties. An indemnity is usually in the form

> "the first party ensures that the second party is held harmless if a particular event occurs".

GITC4 Terms and Conditions clause 22 is an example.

(e) **Third-party guarantees** which address the risk that the supplier may not be able to meet its liabilities by requiring a third party to guarantee that the supplier's liability will be met. An example of a third party guarantee is Schedule 1 of the GITC4 Head Agreement.

9.3 The various contractual arrangements outlined above are usually supported by a contractual requirement that the party allocated a risk must insure against it. Insurance is discussed in detail below.

10. Risk Management and Risk Assessment Process (AS/NZS 4360:2004)

Overview

10.1 The process for estimating an appropriate level of supplier liability under a contract requires an assessment of the risks inherent in the proposed contract (the **Risk Assessment process**). Specifically, an assessment must be made of risks that:

(a) may cause damage to either party if the risks eventuate; and

(b) the Agency is willing, from a policy perspective, to cap.

10.2 The risk assessment process is part of a broader risk management process (see Figure 1: Risk management process below).

10.3 Most Government departments adopt an approach to risk management that is based on Australian/New Zealand Risk Management Standard AS/NZS4360:2004 (the **Standard**). The Standard, which provides a generic guide for managing risk, defines risk in the following two ways:

(a) "exposure to the consequences of uncertainty, or potential deviations from what is planned or expected"[1]; and

(b) "the chance of something happening that will have an impact on objectives".[2]

10.4 More information on the Standard can be found at the Standards Australia website at **www.standards.org.au**.

10.5 The risk management process described in the Standard involves five steps:

(i) establishing the context;

(ii) identifying the risks;

(iii) analysing the risks;

(iv) evaluating the risks; and

(v) treating the risks.

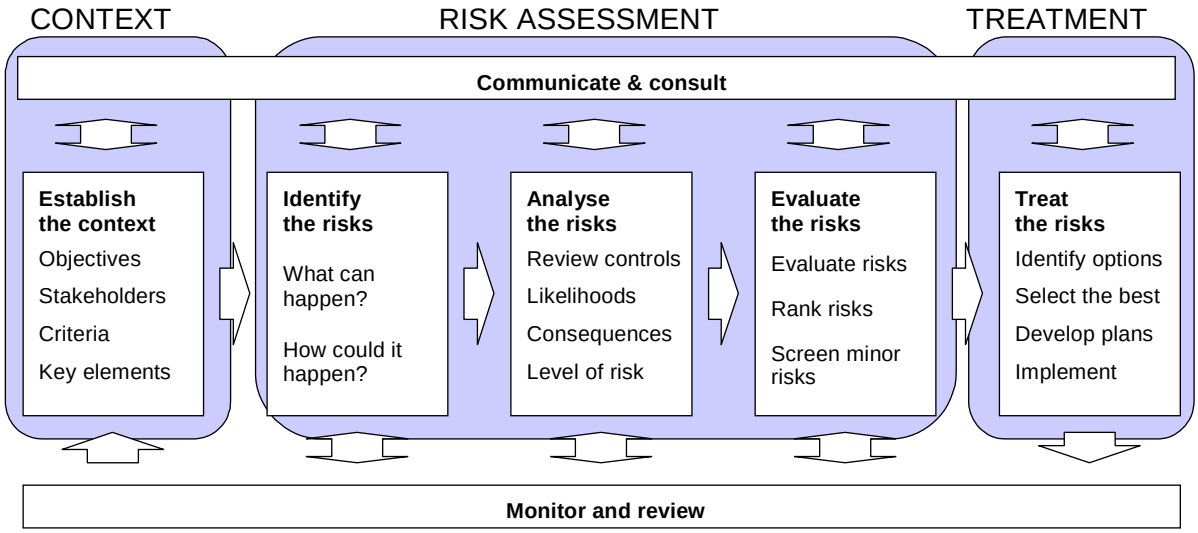
10.6 Throughout the process, there should be consultation and communication with internal and external stakeholders, and ongoing monitoring and review of the effectiveness of each step.

[1] AS/NZS 4360:2004 *Risk Management*, Foreword, p. v.

[2] AS/NZS 4360:2004 *Risk Management*, Definitions, paragraph 1.3.13, p. 4.

10.7 The process is illustrated in Figure 1

Figure 1: Risk management process



10.8 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.

11. Step 1: Establishing the Context of a Risk Assessment

11.1 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 is concerned with understanding the background of the Agency and its objectives in undertaking the procurement.

11.2 There are a number of elements to establishing the Context:

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

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

(c) identifying the criteria by which to measure the success of the contract/procurement; and

(d) identifying the scope of the goods and services to be delivered, including the key elements of those goods and services.

11.3 The Context step of the risk management process is important as it sets the scene for the Identification step and detailed assessment activities that follow. Unless it is done well, the rest of the process is likely to be inefficient.

11.4 It is possible to define the context for a procurement through the development of a Context statement, drawing together the aspects that make up the context of the procurement. The simple Context statement for an example ICT contract may read as follows:

Table 1: Example context statement

Context Part	Description
Objectives	• The contract is to provide 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 organisation • Potential suppliers and preferred tenderer • Supplier sub-contractors • End user within the Agency • The Minister
Criteria	• Technical performance • Financial • Delivery Schedule
Key elements	• Design • Manufacture • Installation and check-out tests • Operation • Maintenance and support

12. Risk Assessment

Step 2: Risk Identification

12.1 The second step in the Risk Management process, and the first step in the Risk Assessment process, is to identify the risks related to the delivery of the goods/services under contract – that is, what events might occur that could frustrate fulfilment of the contract by either party?

12.2 The Risk Identification step has a number of parts:

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

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

(c) identifying who might be affected.

12.3 Risk Identification is crucial to risk assessment, as risks that have not been identified cannot be assessed and mitigated. It is therefore very important that the Risk Identification process be comprehensive. The process should be structured using the key elements developed as part of the Context step to examine risks systematically in each area of the contract scope.

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

"Brainstorming"

12.5 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 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.

12.6 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 people external to the Agency.

12.7 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.

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

> *Supplier may utilise 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.*

Step 3: Risk Analysis

12.9 Once the potential risks have been identified, the next step is to conduct a risk analysis to better understand 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 (see **Appendix 10 – Example Risk Register**).

12.10 A risk analysis can be quite complicated, depending on the procurement activity. Procurement officers are advised to refer to the AS/NZS 436:*2004 Risk Management Guidelines*, which is a companion to the Standard.

12.11 A risk analysis has a number of parts:

(a) evaluating the effectiveness of existing controls;

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

(c) determining the likelihood of the risk eventuating;

Controls

12.12 Any analysis of identified risks must be undertaken with full consideration of existing risk controls. A risk control mitigates the 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 mitigating a risk.

12.13 Existing controls that may be in place for the example risk mentioned at **Paragraph 12.8** include:

(a) Detailed specifications in the contract.

(b) Supplier experience in similar contracts.

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

Consequences

12.14 In a general risk assessment, consequence is 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 that were developed during the context stage (refer **Appendix 8 - Qualitative Measures Of Consequence And Likelihood**).

12.15 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 likelihood of a risk occurring is quantified and expressed numerically in monetary terms.

Likelihood

12.16 In a general risk assessment, likelihood is also described in qualitative terms. A qualitative assessment of likelihood would involve a similar five-point descriptive scale, ranging from a likelihood described as "rare" to one described as "almost certain" (refer **Appendix 8 - Qualitative Measures Of Consequence And Likelihood**).

12.17 However, for the purpose of allocating and estimating liability under the contract a quantitative approach is necessary.

12.18 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 chance of occurring, or one in ten chance. Quantitative assessments like this are important measures against which liability limits may be estimated.

12.19 Assessments of likelihood must consider:

(a) the effectiveness of any existing controls; and

(b) given the controls, what is the probability that this risk will occur.

12.20 The accuracy of a quantitative 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 empirical data, statistics, history, anecdotal evidence and any other relevant sources when making an assessment.

12.21 Where workshop participants are at odds over the likelihood of a risk occurring, it is preferable that the most pessimistic of the estimates of likelihood (i.e. the greater probability, such as 1 in 10, rather than 1 in 100) be accepted. This ensures that there is some level of confidence and margin for error in the final estimate of liability limits.

Risk Analysis Example

For instance, 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.

12.22 The example provided in Table 2 indicates the kind of detail that needs to be captured during the risk identification and risk analysis stages.

Table 2: Example risk

ID #	Risk Description	Controls	Consequence (worst case $)	Likelihood

1.01	Supplier may utilise 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 design features of the system	$75,000	1 in 1,000

Step 4: Evaluate the risks

12.23 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 in their current state or need 'treatment'; and

(b) the order of priority for treating risks assessed as being unacceptable.

12.24 Risk evaluation has a number of parts:

(a) evaluation of the risks;

(b) ranking of the risks; and

(c) screening of minor risks.

12.25 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 **Appendix 8 - Qualitative Measures Of Consequence And Likelihood**).

12.26 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.

13. Step 5: Treatment of the risks

13.1 Treatment of the risks has a number of elements:

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

(b) assessing the preferred risk treatment options; and

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

13.2 When following the risk management process set out in the Standard, strategies for treating the identified risks are developed once the assessment of the risks has been completed.

13.3 Risk treatment involves identifying all legitimate 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 with the potential benefits of mitigating each risk. The preferred options are expanded in detail, responsible officers are allocated the task of managing the risks, and treatment strategies are implemented. Specific provisions may be included in the contract to treat unacceptable risks.

13.4 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 manage the risks. A diverse group of people will introduce a range of possible solutions to the risk, and provide a balanced view in deriving a final risk treatment strategy.

13.5 In respect of allocating liability under the contract, the options are not merely limited to a choice of either (a) agreeing to limit supplier liability or (b) 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 mitigate 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, however, there may be other options to treat risks, such as internal procedures to manage the procurement.

13.6 Treatment strategies may take the form of specific provisions in the contract or sometimes appear as initiatives 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 on that activity. Outside of the contract, the Agency may have identified a risk relating to their ability to effectively manage the contract with the supplier, and the preferred treatment strategy may be the recruitment of a technical specialist to assist in managing the contract and supplier.

13.7 As a general principle, 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 will usually, though not always, be the supplier.

13.8 In addition to allocating and limiting liability, Agencies should be aware that there may also be alternative contractual measures to treat risks, that actively reduce the likelihood and consequence of the risks, prior to estimating liability. This will have the effect of lessening the overall severity of the risks, and hence facilitate a reduction in the level of liability the supplier will be required to accept in the contract. This will in turn reduce the costs for both the supplier and the Agency.

> For example, in the scenario referred to in Table 2, the procurement officer may decide than a reasonable treatment strategy, additional to the existing controls, would be for the supplier to conduct a series of installation tests and checks prior to 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, an order of ten to a one in ten thousand likelihood. This, in turn, may result in a lower limit of supplier liability.

13.9 Table 3 shows how adding further treatment strategies may reduce the likelihood of the risk occurring.

Table 3: Example risk

ID #	Risk Description	Controls	Additional Risk Treatment	Consequence (worst case$)	Likelihood
1.01	Supplier may utilise 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 design features of the system	**Contract to include additional power supply installation test and check requirements**	$75,000	~~1 in 1,000~~ **1 in 10,000**

13.10 The results of the risk assessment, as shown in the example in Table 3, will be used as the basis for the estimate of supplier liability and supplier liability limits. The process of generating liability estimates is discussed in more detail in **Section 16** of this Guide.

14. Conduct of the Risk Assessment

Overview

14.1 The specific nature of the proposed procurement will influence:

(a) how the risk assessment will be undertaken;

(b) the scale of the assessment; and

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

14.2 While the actual form of the risk assessment will be determined by the procurement officer based on the particular circumstances of the procurement, this section provides some guidance on how to make that determination.

14.3 Depending on the nature of the proposed procurement, the risk assessment process can be short and simple or very detailed and complex. The procurement officer undertaking the assessment must consider the value and complexity of the procurement, 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

14.4 The costs of conducting the risk assessment must be weighed against the benefits to be gained. For instance, in a simple contract where the liability risks are considered to be relatively low or easy to calculate, there is little benefit to be gained from spending a large amount of resources in the risk assessment process. On the other hand, complex procurements or high value contracts may require a detailed risk assessment that justifies the commitment of significant resources. In these circumstances, a detailed assessment may be required to ensure that the Agency and supplier are dealt with fairly in relation to liability.

14.5 Procurement officers should note that there will not necessarily be any relationship between the value of the proposed procurement and the magnitude of the liability. That is, a low value procurement may have the potential to cause a high level of damage to a party, and conversely a high value procurement may not have the potential to cause the other party much damage. The magnitude of the liability risk is related to the nature of the procurement and the environment within which it exists, and not the price of the contract. Indeed, the conduct of risk assessments on a procurement considered to be simple may uncover risks and liabilities that warrant more detailed analysis. In such a case, it would be prudent to halt the assessment until specialist support can be obtained.

Key characteristics of ICT procurements

14.6 The complexity of an ICT procurement may be judged by a number of its key characteristics. These include:

(a) software maturity and complexity;

(b) hardware maturity and complexity;

(c) integration requirements and dependency on other systems;

(d) commercial arrangements; and

(e) schedule demands.

Simple procurements

14.7 As a general rule, simple procurements will require simple risk assessments. Referring to the key characteristics listed at **Paragraph 14.6** above, an example of a simple ICT procurement is one that might involve the following characteristics:

(a) the supply of mature software;

(b) the supply of mature hardware;

(c) in a technically routine manner that requires little or no integration or dependency with other systems;

(d) within a basic contractual framework involving few or no subcontractors; and

(e) with a schedule requirement that is achievable.

14.8 When planning for a procurement that meets this description, it would be reasonable to undertake a simple risk assessment. Such an assessment could be conducted quickly and with existing "in-house" resources, possibly drawing on support from a number of specialists.

14.9 However, while a simple risk assessment may have been planned, it may become apparent through the course of the assessment that there are a number of risks that require a more detailed assessment to be conducted.

14.10 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;

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

(c) appropriately allocate liability under the contract.

Complex procurements

14.11 As a general rule, complex procurements will require complex risk assessments. Referring to the key characteristics listed at **Paragraph 14.6** above, an example of a complex ICT procurement is one that might involve one or more of the following characteristics:

(a) developmental software;

(b) developmental hardware;

(c) being integrated into complex and dependent systems;

(d) multiple layers of contractors and sub-contractors providing the services in a complex commercial and contractual framework; and

(e) an aggressive or unrealistic delivery schedule.

14.12 When planning for a procurement that has these characteristics, it would be appropriate to plan for a complex risk assessment, engaging all relevant stakeholders in the risk assessment, and involving subject matter experts as appropriate.

14.13 As with simple procurements, 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;

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

(c) appropriately allocate liability under the contract.

High Value simple procurements

14.14 Technically simple ICT procurements of a high value have the potential to result in significant liability for one or all of the parties due to the overall cost of the procurement.

14.15 For example, a proposed contract to replace all PC monitors in a large Agency may be technically simple and not have any dependency on other systems. However, failure to complete the scope of work to a satisfactory level may result in significant impacts on the client organisation. Because of the high value of the contract, a detailed risk assessment would be appropriate.

High Value complex procurements

14.16 For all high value complex procurements a detailed risk assessment would be appropriate.

15. The supplier

15.1 One element of a risk assessment involves an assessment of the risks of 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 the resources available; and

(d) proposed contractor/sub-contractor arrangements.

15.2 It is not appropriate to assign risk to a supplier merely on the basis of the supplier's size. Small to medium enterprises may represent a low risk strategy if they have good credentials and a sound record in doing the work specified in the contract. Large companies and corporations may also represent a low risk, as they can bring substantial resources and capacity to support complex assignments.

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

Endorsed Supplier

15.4 It is mandatory for FMA Act agencies to use Endorsed Suppliers when purchasing Information Technology (IT) and Major Office Machines (MOM) products and services.

15.5 Risk assessments of proposed ICT contracts involving Endorsed Suppliers should take into consideration the credentials of the supplier and the assessment criteria required to become an Endorsed Supplier. While Endorsed Supplier status may reduce the probability of some liability risks, procurement officers should not rely on this endorsement in assessing the risks of the procurement.

15.6 More information on the Endorsed Supplier Arrangements (**ESA**) may be found at the ESA website at **www.esa.finance.gov.au**

16. Estimating Liability

Overview

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

16.2 A risk assessment for the purpose of estimating and allocating liability should be a quantitative assessment, drawing on the assessment of the likely consequence of a risk eventuating expressed in dollars, and the likelihood of a risk eventuating expressed as a numerical probability, such as a "one in a hundred" or "one in a million".

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

16.4 The starting point for estimating liability is to compile a list of all liability risks, known as a "risk register", that describes:

(a) the risks;

(b) the existing controls;

(c) any additional risk treatments;

(d) the consequence of the risk; and

(e) the likelihood of the risk occurring.

16.5 Maintaining the risk register is an ongoing process, and it should be developed throughout the risk identification, risk analysis and risk evaluation steps described above (see **Appendix 10 – 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 the estimating of liability, and ultimately deciding on an appropriate limit to that liability.

Methods for estimating liability

- **Basic estimate**

16.6 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 identify from the register the risk with the highest value of consequence, and use this as the maximum amount for which the supplier is to be liable under the contract.

16.7 The rationale for this method is that, as it is improbable that more than one of the identified risks will occur through the term of the contract, the highest value risk represents a reasonable upper limit of supplier liability.

16.8 However, if it is considered that 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 estimate**

16.9 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 the damage that may be caused will amount to the summed total of the value of all the risks.

16.10 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.

- **Sophisticated estimate**

16.11 The most sophisticated and accurate, but also the most resource intensive, method of estimating liability is to construct a model that combines:

(a) the financial impact of the consequences; with

(b) the probability of occurrence specified in the likelihood.

16.12 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 risks and liabilities.

16.13 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 what the outputs will provide.

16.14 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.

16.15 Table 4 shows how the risk register might be amended to allow for a sophisticated approach to the liability estimate.

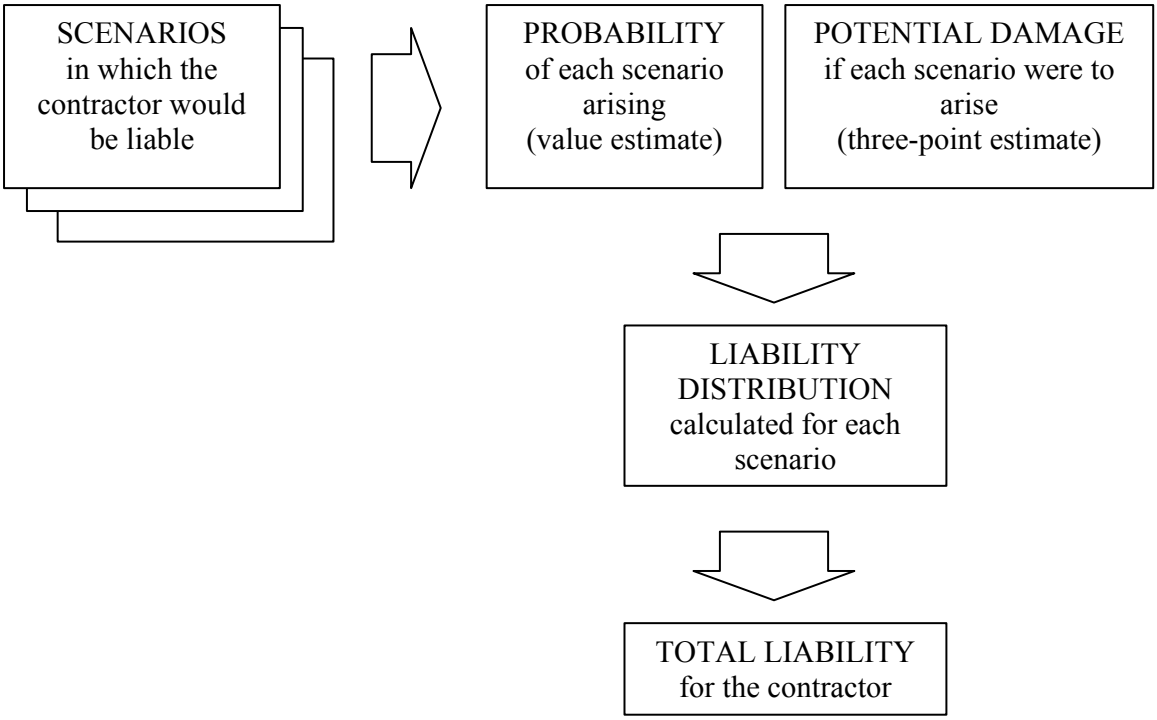
Table 4: Example risk

ID #	Risk Description	Controls	Additional Risk Treatment	Consequence (Best Case Most likely Worst case)	Likelihood
1.01	Supplier may utilise 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 design features of the system	Contract to include additional power supply installation test and check requirements	$1,000 BC $10,000 ML $75,000 WC	~~1 in 1,000~~ **1 in 10,000**

16.16 This method recognises that it is highly unlikely, but not impossible, for more than one risk to occur during the course of the contract. To model the contract risks in a realistic fashion, it is necessary to utilise specialised software that 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. One such simulation application is @Risk for Excel, and a number of other similar packages exist that will perform the same or a similar simulation task.

16.17 A simulation captures data that shows, over a great number of iterations, how risks might occur, based on their probability and consequence. 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. This output is used to determine a level of confidence in the liability exposure of the proposed contract. Figure 2 describes the general process.

Figure 2: Process for developing a liability model



16.18 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 great majority of cases. Through simulating many thousands of possible scenarios, the model will provide data to meet this objective.

16.19 A different approach may be required in relation to "consequential" losses, more accurately known as special or indirect losses. These are losses that would not ordinarily flow from the breach in question, but which are unique to the circumstances and should have been in the contemplation of the parties at the time the breach occurred. Typical examples are loss of revenue, loss of profit and loss of opportunity – in other words, "business losses" which will vary from Agency to Agency.

16.20 Suppliers will often seek to totally exclude liability for "consequential losses" on the basis that they represent a disproportionately high risk relative to the value of the contract. The parties need to adopt a realistic attitude in relation to this subject – Agencies must accept that some IT suppliers will prefer to walk away from a negotiation rather than accept this type of risk, whilst suppliers need to be made aware that the risk can be effectively managed in many instances through a cap on the level of consequential losses without the need for a total exclusion of liability for such losses.

17. Alternative ways to manage risk

Contract Management

17.1 While including appropriate provisions in the contract is an important tool for mitigating and managing risk, the contract is not the only way to mitigate and manage risks. Effective contract management, for example, is also important.

17.2 No matter how complete the contract is in addressing each identified risk, it will not be an effective risk management tool unless is it is well managed. Contract management is the critical process of managing the contract, the interface between client and supplier, and third parties that have rights or obligations under the contract.

17.3 First and foremost, it is very important that the client and supplier organisations provide sufficient resources so that they may meet their obligations under the contract. This means that each party should:

(a) allocate sufficient resources;

(b) provide an adequate and skilled workforce to manage all aspects of the contract; and

(c) provide facilities and other infrastructure that are needed to complete the contract.

17.4 Good contract management also means completing the tasks required of the contract to the greatest extent possible. Performance reviews, reporting and measurement, meetings and audits should all be undertaken in accordance with the contract requirements and in a timely manner. Each of these activities is critical to reducing risks to the contract and will improve the likelihood of a successful procurement outcome.

Identify new risks, monitor and review existing risks

17.5 The risk register is simply a reflection of the identified risks at a point in time in the procurement. Some risks will change over time, some risks may disappear, while new risks may emerge. It is therefore important that all parties implement a process of review to keep the risk register up to date and to manage the risks. This is an important part of good contract management.

17.6 The emergence of new risks, and change in status of existing risks, can dramatically alter the liability estimate and may influence the limit of liability applied to the supplier. Agencies should monitor the risks and liability levels carefully and periodically to ensure that new risks do not increase the financial impact or likelihood of the risks occurring and hence the liability limit.

Contract change or extension

17.7 Amendments to the contract, including increases or reductions to the scope of work or extensions to the contract duration, can cause existing risks to change or new risks to emerge.

17.8 Where there is a proposed amendment to the contract, agencies should review, and where necessary reassess, their risk assessments to understand the nature of any changes to the risk register. This in turn may affect the limit of liability specified in the contract. If the risk assessment indicates that it is possible that liabilities resulting from the occurrence of specific risks may increase, then the limit of liability should be revisited with the supplier. Conversely, a demonstrable reduction in the significance of liability risks may lead to a reduction in the level of liability required.

18. Insurance

Its purpose and limitations

18.1 The purpose of requiring a supplier to hold insurance is to reduce the possibility of the supplier not being able to perform the contract and to ensure that allocations of risk to the supplier are effective. That is, insurance:

(a) can reduce the risk of a supplier not being able to **perform** its obligations under the contract (for example due the destruction of its equipment or premises); and/or

(b) not having the **financial resources** available to meet a liability it incurs under the contract.

18.2 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. In this regard, Comcover ceased to automatically cover contractually assumed risks from 1 July 2004 onwards. The effect being that where an Agency indemnifies, releases or caps a supplier's potential liability, that Agency will 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.

18.3 Procurement officers must consider the availability and cost of insurance in deciding the types and levels of insurance cover required to be held by the supplier. Where a supplier is required to effect insurance specifically for the contract, the cost of such insurance is likely to be fully passed on to the Agency. Requiring unnecessary insurances or insurance for risks that are remote or of low value, may result in unnecessary contract costs.

18.4 Insurance is only one element of a holistic risk management strategy. It addresses the economic consequences of risk, not its physical outcomes (eg. property loss or personal injury). Other forms of risk treatment are also usually required (for example, safe work practices).

Determine what insurance is required

18.5 In order to determine what insurance the supplier should be required to provide, the procurement officer should first consider **what risks will arise** from the performance of the contract or project.

18.6 Secondly, consider **which of the risks to be treated can be insured**. Not all risks are insurable. For example, the risk of a simple non-performance of the contract cannot be insured against.

18.7 Thirdly, for those risks that can be insured, consider **whether insurance is the preferred treatment**. Some risks may be so remote (eg risk of confiscation in Australia), the consequences so catastrophic or the cost of insurance so high (for example, possibly environmental impairment cover) that a decision not to insure may be justified. Another treatment may be more effective or required in addition to insurance. Generally all insured risks should be additionally treated to minimise the chance of the risk occurring and its consequences.

18.8 Fourthly, the advice of an insurance expert should be sought to ensure that the **description** of the insurances required by the insurance provisions in the contract adequately cover the risks intended to be insured. For example, it is a common misconception that a public liability policy will cover liabilities to third parties arising from the supply, manufacture or distribution of a product. In fact, it will not cover such liabilities - a products liability policy is required. For IT services, specialised insurances are required.

Limits of Indemnity

18.9 Consideration should be given as to whether the policies to be effected are required to be **project or contract specific**. If this is not a contractual requirement, then the party required to effect the insurance may rely on policies which cover other business dealings or projects as well as those contemplated by the contract.

18.10 This is not an issue where, for example in respect of a public liability policy, the policy limit is expressed to apply to each and every occurrence. However, where there is an **aggregate limit**, for example under a professional indemnity or product liability policy, a non-project specific policy may be effectively used up by claims unrelated to the contract at the time of a claim arising from the contract.

18.11 To ensure that the limit of indemnity will be available for claims arising in respect of the contract it is prudent to require the insurances which have an aggregate limit to be project or contract specific. Alternatively, a higher aggregate limit of indemnity may provide a level of comfort.

18.12 Contract specific insurance will result in additional costs to the supplier, which costs are likely to be passed on in full to the Agency. Accordingly, care should be exercised in requiring contract specific insurances.

Do not take "no" for an answer

18.13 Insurers, brokers and other contracting parties will often reject contractual insurance obligations or the provision of policy terms initially. However, persistence may result in contractual insurance conditions being met, provided they are reasonable and obtainable in the market at the relevant time.

18.14 Procurement officers should insist on being provided with an opportunity to inspect policy wordings. There is often no legitimate reason why wordings cannot be provided. With respect to professional indemnity insurance, there is usually sensitivity as to limits of liability and the policy may have a confidentiality clause. In such cases, it may be appropriate to accept a certificate of currency showing that the limits and other key terms required by the contract are in force.

A word of caution

18.15 Insurance obligations in contracts should be given thorough consideration early in the negotiation process. Too often these provisions are left until very late in negotiations to be given proper attention, leading to inappropriate terms being agreed to (with parties often being in breach of contract from day one or not being properly protected) or negotiations reaching an unexpected impasse to the frustration of all concerned. Seek advice early on from your insurance advisors as to the appropriateness of draft insurance obligations and the commerciality of suggested terms and amounts. Remember that some policies (particularly contract specific policies) may take some time to place with an insurer.

Appendix 1 – Glossary

CAC Act	means *Commonwealth Authorities and Companies Act 1997.*
CAC Regulations	means *Commonwealth Authorities and Companies Regulations 1997*.
CAC Act Body	means a body that is subject to the *Commonwealth Authorities and Companies Act 1997*.
CPGs	means the Commonwealth Procurement Guidelines January 2005.
Endorsed Supplier	means a supplier who is pre-qualified under the ESA.
ESA	means the Australian Government's Endorsed Supplier Arrangement which provides pre-qualification for businesses in the Information Technology, Major Office Machines, Commercial Office Furniture and Auctioneering industries to sell to the Australian Government.
FMA Act	means the *Financial Management and Accountability Act 1997*.
FMA Act Agency	means an Agency that is regulated by the *Financial Management and Accountability Act 1997.*
FMA Regulations	means the *Financial Management and Accountability Regulations 1997.*
GITC4	means version four of the Australian Government Information Technology and Communications contract version 4 available at www.gitc.finance.gov.au. GITC is a set of legal documents used by government to create contracts for the purchase of information technology goods and services.
ICT	means information and communications technology.
ICT Liability Policy	means the Australian Government's policy that FMA Act Agencies should, in most cases, cap the liability of ICT suppliers at appropriate levels and approved by the Minister for Finance and Administration and the Minister for Communication, Information Technology and the Arts on [insert date] 2005.
IP	means Intellectual Property.
Risk assessment	means the overall process of risk identification, risk analysis and risk evaluation. Its purpose is to develop agreed priorities for the

	identified threats and opportunities.
Risk identification	means the process of determining what, where, when, why and how something could happen.
Risk analysis	means the systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
Risk evaluation	means the process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Consequence	means 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.
Likelihood	means a qualitative description of probability or frequency

Appendix 2 – ICT Liability Policy

(DRAFT) Finance Circular

No. <<Year/xx>>

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 [3] (ICT) contracts.

This Circular is effective from ….

(b) Target Audience

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

The Policy

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 continue to be required as part of ICT contracts when they are justified by the size, complexity or inherent risk of a project.

Context

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

[3] 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.

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.

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.

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

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.

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

Background

1. The *Commonwealth Procurement Guidelines* (CPGs) set out the Australian Government's policy on procurement, including its overarching policy on risk management. The CPGs provide that:
   - 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.

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

Applying the Policy

3. 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 (CFO) 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.

4. 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).

5. 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

6. Agencies' decisions when approving a spending proposal, including whether to cap liability, or require unlimited liability, must be fully documented in accordance with FMA Regulation 12.

1.1 Additional Resources

7. 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, *A Guide to Limiting Supplier Liability in Information and Communications Technology (ICT) Contracts for Australian Government Agencies*.
   - *Commonwealth Procurement Guidelines – January 2005*.
   - Finance Circular 2003/02 *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort.*
   - Finance Circular 2004/10 *Using the Financial Management and Accountability Regulation 10 Delegation*.

Contacts

8. Questions should be directed to the Procurement Agency Advice Branch at procurementagencyadvice@finance.gov.au or visit our website at http://www.finance.gov.au (under the Government Finances menu).

Jonathan Hutson
Division Manager
Financial Framework Division
Financial Management Group
<<Date>> <<Month>> <<Year>>

Appendix 3 – Table of liabilities for ICT contracts.

1. Characterisation of Supplier Liability

1.1 The ICT Liability Policy provides that the liability of ICT suppliers contracting with FMA Act Agencies should, in most cases, be capped at appropriate levels.

1.2 To assist in determining whether or not particular supplier liabilities should be unlimited or capped, Australian Government contracts have traditionally characterised supplier liabilities in the following two ways:

- ***Supplier liability characterised by the activity that leads to the liability (Activity Based Supplier Liability)***

  Activity Based Supplier Liability is a supplier's liability to compensate the Commonwealth for **all** damage or loss suffered by the Commonwealth, directly or indirectly (see the explanation of direct and indirect damages in 1.3 below), **as a result of the supplier's activities**. For this category of liability, consideration of whether or not to cap the supplier's liability focuses on the particular *activity* that might cause the damage, and not on the *types of damage or losses* that may arise.

  Examples of *Activity Based Supplier Liability* include supplier liability that arises as a result of:

  - the supplier breaching its IP, confidentiality or privacy obligations; and
  - the supplier breaching its service delivery obligations.

- ***Supplier liability characterised by the damages that arise (Damage Based Supplier Liability)***

  Damage Based Supplier Liability is a supplier's liability to compensate for particular **types of damage**, whether direct or indirect (see the explanation of direct and indirect damages in 1.3 below), that may result from the act or omission of a supplier. For this category of liability, consideration of whether or not to cap the supplier's liability focuses on the *types of damage or losses* that may arise, irrespective of the supplier *activity* that caused the damage.

Examples of *Damage Based Supplier Liability* include supplier liability for:

- property damage; and
- personal injury and death.

1.3 The explanation of Activity Based Supplier Liability in paragraph 1.2 refers to the "supplier's liability to compensate the Commonwealth for all damage or loss suffered by the Commonwealth, directly or indirectly" and the explanation of Damage Based Supplier Liability also in paragraph 1.2 refers to the "supplier's liability to compensate for particular types of damage", whether "direct or indirect".

1.4 The characterisation of losses as being "direct" or "indirect" (or otherwise) is a complex legal issue as there is no precise definition for "direct loss", "indirect loss" or "damage". For the purposes of explaining approaches to capping liability, this Guide has adopted the following simple descriptions of "direct" or "indirect" liabilities or losses:

(a) a "direct" liability or loss means that a supplier causes loss to an Agency which flows naturally, and could be expected to flow in the usual course of things, from the supplier's breach. An example is where the supplier causes damage to Commonwealth property or fails to supply a deliverable which has been the subject of prior payment or part payment; and

(b) an "indirect" liability or loss means that a supplier causes loss which would not normally arise in the usual course of things but which has nevertheless arisen as a consequence of the supplier's breach in unique circumstances where the supplier had reasonable prior knowledge that such a loss might occur. Such losses might include an Agency's resultant liability to a third party. An example of the former is where an agency is deprived of revenue due to a defect in a new IT system. An example of the latter is where a supplier's failure to ensure proper licensing arrangements in relation to IP causes an IP owner to claim against the Commonwealth for IP infringement.

1.5 The issue is made more complex by the fact that different jurisdictions use different terminology and characterise damages in different ways – an issue which Agencies must be particularly wary of when negotiating liability caps with suppliers from other countries. In particular, legal advice should be sought before either:

(a) inserting a definition of loss into the contract (and therefore ceasing to use the approach in GITC 4 which relies on the meaning of loss under the common law); or

(b) amending the definition of loss that is commonly used in Australian Government contract precedents, which defines "Loss" or "Losses" to mean any loss, damage (whether direct or indirect), liability, cost or expense, including legal expenses on a solicitor and own client basis.

2. Treatment of the types of Supplier Liability

2.1 The table below lists the types of Activity Based Supplier Liability and Damage Based Supplier Liability that are commonly identified in Commonwealth ICT contracts. The table also identifies which of the liabilities are commonly left unlimited, which are commonly capped, and how the ICT Liability Policy might apply to each of the liabilities.

2.2 Due to the fact that Commonwealth contracts do not use one proforma supplier indemnity (and as GITC 4 is under review), the table does not consider or describe supplier liabilities in terms of some of the commonly used indemnity provisions.

2.3 A reference in the table to a "cap" may embrace a situation in which direct losses are capped whilst indirect losses are totally excluded, although this will not necessarily be the case and will be subject to negotiation in each instance.

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
ALL TYPES OF DAMAGE							
Current Cth practice	tends to require unlimited supplier liability but sometimes caps.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to be silent on the issue of liability.	tends to require unlimited supplier liability but sometimes caps.	tends to require unlimited supplier liability.
GITC 4 position on supplier liability	allows capping for breach of contract but discourages capping for breach of IP, confidentiality and privacy obligations; third party damage caused by negligent act or omission, or wilfully wrongful or unlawful conduct and for property damage and personal injury.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	is silent on the issue of liability arising from breach.	allows capping for negligent act or omission, but discourages capping for breach of IP, confidentiality and privacy obligations; third party damage caused by negligent act or omission, or wilfully wrongful or unlawful conduct and for property damage and personal injury.	allows capping for wilfully wrongful or unlawful conduct, but discourages capping for breach of IP, confidentiality and privacy obligations; third party damage caused by negligent act or omission, or wilfully wrongful or unlawful conduct and for property damage and personal injury.
Capping recommendation	Should cap at appropriate levels, subject to other recommendations re unlimited liability	Only cap if there is a compelling reason valid policy reasons for continuing to require suppliers to accept unlimited liability.	Only cap if there is a compelling reason valid policy reasons for continuing to require suppliers to accept unlimited liability.	Only cap if there is a compelling reason - valid policy reasons for continuing to require suppliers to accept unlimited liability.	Only cap if there is a compelling reason valid policy reasons for requiring suppliers to accept unlimited liability.	Should cap at appropriate levels, subject to other recommendations re unlimited liability.	Only cap if there is a compelling reason - valid policy reasons for requiring suppliers to accept unlimited liability.

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
Tangible Property damage	Supplier breach of service delivery obligations may cause damage to tangible property.[i]	Supplier breach of IP obligations unlikely to cause damage to tangible property.	Supplier breach of confidentiality obligations unlikely to cause damage to tangible property.	Supplier breach of privacy obligations unlikely to cause damage to tangible property.	Supplier breach of security obligations could cause damage to tangible property. [ii]	Supplier negligent act or omission could cause damage to tangible property.[iii]	Supplier wilful or unlawful conduct could damage to tangible property[iv].
Current Cth practice	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.
GITC 4 position on supplier liability	unlimited supplier liability for property damage arising from breaches of service delivery obligations is the default position.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	is silent on the issue of liability arising from breach but default position requires unlimited supplier liability for property damages arising from breaches of security obligations.	unlimited supplier liability is the default position	unlimited supplier liability is the default position
Capping recommendation	Only cap if there is a compelling reason Comcover unlikely to provide building and contents insurance for losses above cap.	Only cap if there is a compelling reason	Only cap if there is a compelling reason.	Only cap if there is a compelling reason.	Only cap if there is a compelling reason	Only cap if there is a compelling reason Comcover unlikely to provide building and contents insurance for losses above cap.	Only cap if there is a compelling reason valid policy reasons for requiring unlimited liability.

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
Economic loss[v]	Supplier breach of service delivery obligations could cause economic loss.[vi]	Supplier breach of IP obligations could cause economic loss. [vii]	Supplier breach of confidentiality obligations could cause economic loss[viii].	Supplier breach of privacy obligations could cause economic loss.[ix]	Supplier breach of security obligations could cause economic loss.	Supplier negligent act or omission could cause economic loss.[x]	Supplier wilful or unlawful conduct could cause economic loss.
Current Cth practice	tends to require unlimited supplier liability or is silent on the issue.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability or is silent on the issue.	tends to require unlimited supplier liability.
GITC 4	allows capping for economic loss; but default position is unlimited liability for breach of IP, confidentiality and privacy obligations.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	allows capping for economic loss arising from breaches of security obligations; but default position is unlimited liability for breach of IP, confidentiality and privacy obligations.	allows capping for economic loss; but default position is unlimited liability for breach of IP, confidentiality and privacy obligations.	allows capping for economic loss; but default position is unlimited liability for breach of IP, confidentiality and privacy obligations.
Capping recommendation	Should cap at appropriate levels economic loss arising from breach of service delivery obligations	Only cap if there is a compelling reason.	Only cap if there is a compelling reason.	Only cap if there is a compelling reason.	Only cap if there is a compelling reason.	Should cap at appropriate levels economic loss arising from negligent act or omission.	Only cap if there is a compelling reason.

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
Cost of fixing defects in performance of contract *(std breach of contract damages)*	Supplier breach directly results in Cth incurring the cost of fixing defects in performance of contract.[xi]	Supplier breach of IP obligations could cause this type of loss.	Supplier breach of confidentiality obligations could cause this type of loss	Supplier breach of privacy obligations could cause this type of loss.	Supplier breach of security obligations could cause this type of loss.	Supplier negligent act or omission could cause this type of loss.	Supplier wilful or unlawful conduct could cause this type of loss.
Current Cth practice	tends to require unlimited supplier liability but sometimes caps.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	Cth tends to require unlimited supplier liability.	tends to be silent on the issue of liability.	tends to require unlimited supplier liability but sometimes caps.	tends to require unlimited supplier liability.
GITC 4	allows capping cost of fixing defects; default position is unlimited liability for breach of IP, confidentiality and privacy obligations.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	allows capping cost of fixing defects; default position is unlimited liability for breach of IP, confidentiality and privacy obligations.	allows capping cost of fixing defects; default position is unlimited liability for breach of IP, confidentiality and privacy obligations.	allows capping cost of fixing defects; default position is unlimited liability for breach of IP, confidentiality and privacy obligations.
Capping recommendation	Should cap at appropriate levels cost of fixing defects.	Only cap if there is a compelling reason.	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Should cap at appropriate levels, subject to other recommendations re unlimited liability.	Only cap if there is a compelling reason valid policy reasons for requiring unlimited liability.

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
3P claim for personal injury including sickness and death, breach of IP, breach of confidentiality or breach of privacy	Supplier breach of service delivery obligations may cause personal injury including sickness and death.[xii]	Supplier breach of IP obligations unlikely to cause personal injury including sickness and death.	Supplier breach of confidentiality obligations unlikely to cause personal injury including sickness and death.	Supplier breach of privacy obligations unlikely to cause personal injury including sickness and death.	Supplier breach of security obligations may cause personal injury including sickness and death	Supplier negligent act or omission may cause personal injury including sickness and death.	Supplier wilful or unlawful conduct may cause personal injury including sickness and death.
Current Cth practice	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.
GITC 4	unlimited supplier liability for personal injury arising from breaches of service delivery obligations is the default position.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	is silent on the issue of liability arising from breach; default position is unlimited supplier liability for personal injury arising from breaches of security obligations.	unlimited supplier liability is the default position	unlimited supplier liability is the default position
Capping recommendation	Only cap if there is a compelling reason valid policy and legislative reasons for requiring unlimited liability.	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
Tangible Property damage	Supplier breach of service delivery obligations may cause third party property damage.[xiii]	Supplier breach of IP obligations unlikely to cause third party tangible property damage.	Supplier breach of confidentiality obligations unlikely to cause property damage.	Supplier breach of privacy obligations unlikely to cause property damage	Supplier breach of security obligations could cause property damage	Supplier negligent act or omission could cause property damage.	Supplier wilful or unlawful conduct could cause property damage
Current Cth practice	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.
GITC 4	unlimited supplier liability for property damage arising from breaches of service delivery obligations is the default position.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	silent on the issue of liability arising from breach; default position is unlimited supplier liability for property damages arising from breaches of security obligations.	unlimited supplier liability is the default position	unlimited supplier liability is the default position
Capping recommendation	Only cap if there is a compelling reason Comcover unlikely to provide building and contents insurance for losses that are above liability cap.	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason Comcover unlikely to provide building and contents insurance for losses that are above liability cap.	Only cap if there is a compelling reason Comcover unlikely to provide building and contents insurance for losses that are above liability cap.

SUPPLIER ACT/ OMISSION RESULTING IN LIABILITY → / TYPE OF DAMAGE SUFFERED BY AGENCY ↓	Breach of contract obligations					Negligent act or omission	Wilfully wrongful or unlawful conduct
	Service delivery obligations	IP obligations	Confidentiality obligations	Privacy obligations	Security obligations		
3P negligence claim for other economic loss[xiv]	Supplier breach of service delivery obligations may cause other economic loss	Supplier breach of IP obligations may cause other economic loss	Supplier breach of confidentiality obligations may cause other economic loss	Supplier breach of privacy obligations unlikely to cause other economic loss.	Supplier breach of security obligations may cause other economic loss	Supplier negligent act or omission may cause other economic loss.	Supplier wilful or unlawful conduct may cause other economic loss
Current Cth practice	tends to require unlimited supplier liability or is silent on the issue.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability.	tends to require unlimited supplier liability or is silent on the issue.	tends to require unlimited supplier liability.
GITC 4	allows capping supplier liability for third party economic loss except if arising from breach of IP, confidentiality and privacy obligations, negligent act or omission or wilfully wrongful or unlawful conduct.	unlimited supplier liability is the default position.	unlimited supplier liability is the default position	unlimited supplier liability is the default position	requires unlimited supplier liability.	requires unlimited supplier liability for third party damages arising from negligent act or omission.	requires unlimited supplier liability for third party damages arising wilfully wrongful or unlawful conduct.
Capping recommendation	Should cap at appropriate levels.[xv]	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Only cap if there is a compelling reason	Should cap at appropriate levels, except loss arising from breach of IP, confidentiality, privacy, & security obligations or wilfully wrongful or unlawful conduct.	Only cap if there is a compelling reason valid policy reasons for requiring suppliers to accept unlimited liability.

[1] Eg. hardware malfunction (faulty CRT monitor) starts fire and burns down Cth building.

[1] Eg. physical security breaches could involve, or lead to, breaking and entering and could cause property damage.

[1] Eg. MAC services improperly performed by technician, causing property damage in the course of the MAC.

[1] Eg. drunk service provider personnel drives vehicle into Cth building.

[1] Examples of economic loss includes rent on damaged building, of productivity

[1] Eg. hardware malfunction (eg faulty cable or CRT monitor) means Agency needs to rent new premises to work from and loss of productivity.

[1] Eg. if the IP is not available as contracted (i.e. because 3rd party holds all the IP rights), cost of procurement of the withheld IP or alternative IP is an economic loss.

[1] Eg. breach could result in loss of commercial value of the protected info and costs of investigation.

[1] Eg. costs of investigation of breach might arise.

[1] Eg. failure to maintain server prevents Cth officers from working.

[1] Eg. incorrect input of data requires re-input of data, fixing up flow-on effects of incorrectly entered data.

[1] Eg, Hardware malfunction (eg faulty power supply/cable or CRT monitor) sets fire killing inhabitants or causing noxious fumes inhalation.

[1] Eg. hardware malfunction (eg faulty power supply/cable or CRT monitor) sets fire burning down landlord's building,

[1] Economic Loss not consequential on personal injury, death or property damage. Courts are reluctant to find a duty of care in such cases and therefore these damages are not commonly awarded.

Appendix 4 - Proforma Liability Capping Clauses

1. INDEMNITY

1.1 Indemnity by supplier

Unless specified to the contrary in the Contract Details, the Supplier will indemnify the Agency (including its Personnel) against a loss (including reasonable legal costs and expenses) or liability that has been reasonably incurred by the Agency arising from:

(a) any suit, action or proceeding by any person[4] where that loss or liability was caused or contributed to by an unlawful or wilfully wrong act or omission by the Supplier or its Personnel; or

(b) a claim made or threatened against the Agency in which it is alleged that a Service or Product (including the Agency's use of a Service or Product) infringes the Intellectual Property Rights of a third party. For the purposes of this **clause [1.1(b)]**, an infringement of Intellectual Property Rights includes unauthorised acts which would, but for the operation of the *Patents Act* 1990 (Cwlth) s.163, the *Designs Act* 1906 (Cwlth) s.40A, the *Copyright Act* 1968 (Cwlth) s.183 and the *Circuits Layout Act* 1989 (Cwlth) s.25, constitute an infringement.

1.2 Agency's obligations to supplier

Where the Agency wishes to enforce an indemnity described in **clause [1.1]**, it must:

(a) give written notice to the Supplier as soon as practicable;

(b) subject to the Supplier agreeing to comply at all times with government policy relevant to the conduct of the litigation, including but not limited to any specific obligations set out in the Contract Details, permit the Supplier, at the Supplier's expense, to handle all negotiations for settlement and, as permitted by law, to control and direct any litigation that may follow; and

[4] This is broader than the current GITC 4 which restricts the indemnity to claims by third parties.

(c) in the event that the Supplier is permitted to handle negotiations or conduct litigation on behalf of the Agency, provide all reasonable assistance to the Supplier in the handling of any negotiations and litigation.[5]

1.3 Conduct of Litigation

Unless stated to the contrary in the Contract Details, the Supplier will comply with the following provisions of the Commonwealth Attorney-General's Legal Services Directions issued under section 55ZF of the Judiciary Act 1903 (Cwlth) (in this clause referred to as the 'Legal Services Directions') as if the Supplier were the Agency:

(a) paragraph 4.2 and Appendix B – which provide that claims are to be handled and litigation is to be conducted as a model litigant;

(b) paragraph 4.3 – which provides that claims and litigation are to be conducted in accordance with legal principle and practice (as that expression is amplified in paragraph 2 of Appendix C to the Legal Services Directions);

(c) paragraph 8 – which requires reliance on statutory limitation periods unless approval otherwise is given. [6]

1.4 Supplier's Obligation to Agency

The Supplier will:

(a) keep the Agency informed of any significant developments relating to the conduct of the defence of any claim; and

(b) provide to the Agency such information and documentation as are reasonably requested by the Agency, to enable the Agency to ascertain whether the defence by the Supplier of any claim is being conducted in accordance with the provisions of the Legal Services Directions, including information and documentation covered by legal professional privilege or any other confidentiality obligation.[7]

---

[5] This subclause reiterates the existing wording of GITC4.

[6] This subclause is not in the current GITC4. It has been introduced to take account of the Commonwealth's model litigant obligations in circumstances where the Supplier is to conduct litigation under the Commonwealth's name.

[7] This flows from the new subclause 3.

1.5 Continued Use or Replacement of Infringing Material

If a claim of infringement of Intellectual Property Rights is made or threatened by a third party, the Agency will allow the Supplier, at the Supplier's expense, to either:

(a) obtain for the Agency the right to continued use of the Service or Product; or

(b) replace or modify the Service or Product so that the alleged infringement ceases so long as the Service or Product continues to provide the Agency with equivalent functionality and performance as required in the Specifications.[8]

1.6 Survival of Clause

Clause 22 will survive the termination and expiry of this Contract.[9]

[8] This is the GITC4 wording.

[9] Note that this recommended Indemnity clause does not include the option for the Supplier to require an indemnity from the Customer, in contrast to GITC4.

2. LIABILITY

2.1 Relevant Law

The liability of either party for breach of this Contract or for any other common law or statutory cause of action arising out of the operation of this Contract will be determined under the relevant law in Australia that is recognised, and would be applied, by the High Court of Australia.[10]

2.2 Limitation

If so specified in the Contract Details, liability arising under this Contract will be capped.[11] Unless expressly stated otherwise in the Contract Details, the cap on liability specified in the Contract Details[12] will apply for the benefit of both parties in respect of each single occurrence or a series of related occurrences arising from a single cause[13]. Except as otherwise provided in the Contract Details, this limitation does not apply to liability for:

(a) personal injury, including sickness and death;

(b) loss of, or damage to, tangible property[14];

(c) an indemnity in respect of third party claims under **clause [XX];**

(d) infringement of Intellectual Property Rights;

(e) a breach of an obligation of confidentiality;

(f) a breach of an obligation of privacy;

---

[10] This subclause is in the existing GITC4.

[11] It is desirable, where a cap exists, to ensure the Commonwealth has a right of termination in circumstances where the cap is reached and the Commonwealth has no prospect of receiving further damages in the event of future breaches.

[12] The cap is generally a multiple of the contract price. It is preferable to specify a dollar figure where possible in order to avoid any ambiguity.

[13] This is a "per occurrence" cap. Suppliers will prefer an aggregate cap. Whether this is reasonable or not should be a matter for negotiation.

[14] Property damage may be sub-categorised into "Commonwealth property" and "third party property". The Commonwealth may agree to including Commonwealth property within the agreed liability cap, or negotiating a separate and higher cap for Commonwealth property, but third party property damage should remain outside the cap.

(g) loss of data; or[15]

(h) the payment of any monies due under the Contract[16].

2.3 Review of Liability Cap

The Parties acknowledge that the liability cap set out in this Contract will be subject to review in the event that the Contract is varied or extended. For the avoidance of doubt, a Party may require a review of the liability cap as a condition of its agreement to a change request but only for the purpose of achieving a proportionate adjustment to reflect any alteration to that Party's risk exposure arising out of the Contract variation[17].

2.4 Indirect Losses

Unless stated to the contrary in the Contract Details, a Party will not be liable to the other Party in contract or tort for, or in respect of, any special, indirect or consequential loss or damage suffered by the other Party (including loss of profit, loss of revenue, loss of goodwill, loss of opportunity or any similar financial loss)[18] arising out of or in connection with or relating to the performance of its obligations under this Contract, even if the Supplier is aware or to be aware that such loss is likely to be incurred[19].

[15] This is likely to be contentious. Suppliers are more likely to seek total exclusion of liability in respect of "loss of data". This is an issue which requires negotiation in each instance, with due regard being given to the risks and responsibilities confronting each party.

[16] This is clearly to the Supplier's advantage but seems both reasonable and logical.

[17] This is a difficult concept to mandate contractually. Nevertheless the theory is that (a) once the parties have agreed upon a liability cap, that cap should remain in place, and (b) in the event of a contract variation which affects the scope or price of the contract, it may be appropriate to review the appropriateness of the original liability cap but only to the extent that a party's risk may have altered as a result of the contract variation.

[18] Care should be taken not to extend the categories in parenthesis, particularly an attempt by the Supplier to include generalised events such as "loss of data" or "business interruption".

[19] This approach contrasts to GITC 4 which makes an exception to the exclusion of liability for consequential losses in circumstances where "the Supplier is aware or ought to be aware that such loss is likely to be incurred" – as the essence of "consequential loss" is that the loss is one which, whilst unique to the circumstances, is one of which the parties should have been aware, the GITC 4 qualification effectively negates the exclusion and is of little benefit to suppliers.

2.5 Contributory Negligence

The liability of a party ('the party at fault') for loss or damage sustained by the other party will be reduced proportionately to the extent that such loss or damage has been caused by the other party's failure to comply with its obligations and responsibilities under this Contract and/or to the extent that the negligence of the other party has contributed to such loss or damage, regardless of whether a claim is made by the other party for breach of contract or for negligence[20].

2.6 Consequences of Provision of Faulty Data by Agency

The Supplier will not be held accountable for a failure to meet its contractual obligations to the extent that the failure is attributable to the provision by the Agency of inaccurate or incomplete information which is required by the Supplier for the purposes of the Contract. The Supplier must notify the Agency as soon as practicable if it becomes aware that the provision by the Agency of incomplete or inaccurate information in any instance might prevent the Supplier from complying with its obligations under this Contract.

2.7 Right of Offset

Unless specified to the contrary in the Contract Details, the Agency has a right to offset any proven entitlement to damages against the price applicable to Services or Products subsequently supplied under this Contract or against any amount owing by the Agency to the Supplier under any other contract[21].

2.8 Liquidated Damages

If an amount has been specified in the Contract Details as an amount which is payable as and by way of liquidated damages in respect of specified events[22], the Supplier must pay such liquidated damages within 5 working days of written demand by the Agency in the event that such damages become payable. The payment of liquidated damages by the Supplier will discharge the Supplier's liability arising out of the act or omission giving rise to the payment of such damages but, unless stipulated to the contrary in the Contract Details:

---

[20] The intent of this clause is to overcome the common law principle that a reduction in damages for contributory negligence is not available in circumstances where the action is brought for breach of contract, and not in tort.

[21] The latter qualification may be unacceptable to the Supplier and can be dispensed with under negotiation.

[22] Care must be taken to ensure that the amount specified by way of liquidated damages is a reasonable estimate of losses likely to be incurred as a result of the event in question. If the sum is set at too low a figure, the Customer will have denied itself suitable compensation; if the figure is set too high, the clause may be unenforceable on the grounds that it will be deemed by a court to be a "penalty".

(a) will not prevent Agency from terminating the Contract if a continuation of the specified events gives rise to a right of termination and, in such circumstances, the Agency may pursue an entitlement to damages arising out of the termination[23]; and

(b) will not be taken into account for the purposes of quantifying damages which are subject to any liability cap applicable to this Contract[24]. The operation of this clause may be expressly varied in the Contract Details.

2.9 Survival of this Clause

This clause will survive the termination or expiry of this Contract.

[23] Liquidated damages traditionally apply to delays. It is important that the Customer retains a right to terminate for a protracted delay, not merely to seek liquidated damages. If the Customer does terminate, its entitlement to damages will most likely exceed what it has recovered by way of liquidated damages to date.

[24] This is likely to be contentious and may have to be the subject of negotiation with the Supplier.

Appendix 5 - Procurement Process Timeline

1. Timing for Conduct of Assessment of Risk and Liability

1.1 A common question in the course of undertaking procurement is "when is the best time to conduct the assessment of liability?" As has been 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.

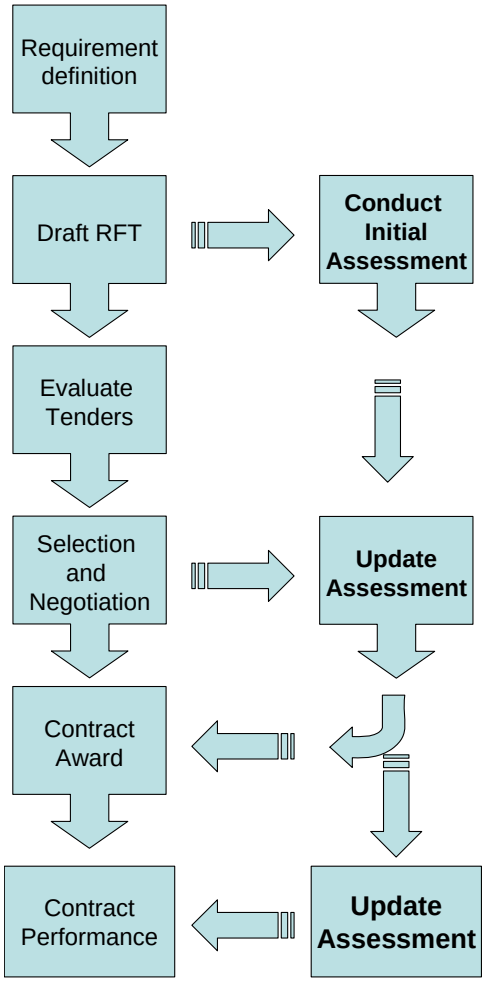
1.3 Draft RFT. Procurement officers should conduct a preliminary assessment of risk and liability prior to, or at the same time as, the tender documentation (RFT; REOI etc) is being drafted. This allows procurement officers to convert treatment strategies developed in response to the assessment of risks into contract provisions and conditions of the tender. Using the early risk assessments, the procurement officers can start to build up a picture of the liability risks and their general value. This value can be communicated to industry as an initial estimate of liability limits in the draft contract included in the RFT.

1.4 Source Selection and Contract Negotiation. Once a preferred tenderer is selected and contract negotiations commence, the procurement officer will have a better idea of the risks to the procurement, based on the suppliers 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.

1.5 Contract Performance. As mentioned in **Section 17** of this Guide, 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 may 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.

Figure 3 illustrates the recommended assessment points against a generic procurement timeframe. Procurement officers should not be limited by this example and are encouraged to plan for an assessment program that best suits their requirements and the nature of the procurement activity.

Figure 3: Contract and risk assessment schedule


Requirement definition
Draft RFT
Conduct Initial Assessment
Evaluate Tenders
Selection and Negotiation
Update Assessment
Contract Award
Contract Performance
Update Assessment

Appendix 6 – Case Studies

This Appendix considers 5 case studies to illustrate how the practices described in this Guide can be applied in an ICT procurement.

Case Study 1 - Purchase of flat-screen LCD monitors to replace conventional monitors

Background

An Agency has a requirement to replace all conventional CRT-type monitors with flat screen equivalents. The estimated cost of the procurement is above $80,000. The Agency will issue an RFT requesting Endorsed Suppliers to quote to supply the monitors. (Installation of the monitors is estimated to cost less than $80,000 and will occur under a separate work order issued to the Agency's existing IT support services provider panel.)

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 tenderer's 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 GITC4, amended to include liability clauses similar to the provisions set out in Appendix 4. The RFT stated that respondents were to indicate compliance or otherwise with the clauses and specify a proposed liability cap.

Evaluation of Tenders

The preferred tender offered a new type of flat screen (**innovative flat screen**) that was assessed by the evaluation committee as demonstrating improvements in performance at a significantly lower total cost of $2,000,000, 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.

Conduct of further Risk Assessment to address specifics of Tenders

As part of the tender evaluation phase, a further risk assessment was undertaken of the tendered solutions. 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 flat screen including:

1. possible delays in production and delivery of the large quantity of screens required by the Agency;

2. possible poor reliability and screen failures well before the anticipated end of life; and

3. shortage of spares and support equipment after installation while the supplier is building up its support capability.

The assessment found that the probability of there being 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 costs to the Agency of these risks occurring was also 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.

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 mitigation 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 alternate 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, minimum reliability performance and mandated levels of spares holdings and support capability.

The procurement officer cited and kept a copy of all insurances that the RFT and contract required the supplier to hold.

The Installation Contract

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 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 1 in 100. The likelihood of more than one risk eventuating and the combined damages exceeding more than $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 property (including the screens).

Case Study 2 - Installation of a network, with normal business applications, in a new Agency facility

Background

An Agency is building a new facility and, as part of the fit-out prior to occupation, must install a computer network, including all infrastructure, file servers, switching, work stations and basic applications. The Agency is seeking to appoint one supplier who will be responsible for the installation work, as well as for provision of network support for the first three years following installation. The estimated cost of the procurement is above $80,000 (in the range of $750,000). The Agency will issue an RFT requesting Endorsed Suppliers to quote to provide the services.

Preliminary Risk Assessment and Preparation of RFT

The procurement officer prepared a Context Statement (similar to the statement in Table 1) to assist the officer to identify key project objectives, stakeholders and evaluation criteria. The procurement officer's initial view was that the procurement was a borderline simple/complex procurement and 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 at Table 2) by considering each key aspect of the scope of work. The procurement officer used the consequence scales and likelihood ratings in tables 1 and 2 in Appendix 8 to qualitatively rank or assess the risks.

The risk assessment found that, in view of contemporary building standards and IT requirements, the scope of work did not carry any risks with moderate to severe consequences that were likely to eventuate. The stakeholders did, however, identify risks associated with a single supplier conducting the full scope of work, given that this covered a variety of difference services ranging from design and installation of the physical IT infrastructure of the facility to delivery of a network service to end users. Stakeholders considered that a number of major sub-contractors would be needed to support the supplier. The main risks identified by stakeholders were:

1. poor sub-contractor management by the supplier may lead to delays in the installation and slippage in the required Agency occupation date; and

2. poor through-life support of the network due to multiple and complicated sub-contractor arrangements.

The risk of poor sub-contractor arrangements impacting adversely on the project were 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 were assessed as major as the financial impact on the Agency of not being able to occupy the facility on the required date was significant.

Limit of Liability

The procurement officer and stakeholders estimated that the occupancy date for the Agency may slip by as much as 30 days while initial network problems were resolved, and this would cost the Agency $100,000 in additional rental costs in existing facilities. Poor through life network support would not cost the Agency much in easily quantifiable financial terms but would reduce the organisations efficiency while the problems were being resolved.

The procurement officer included liability clauses similar to those in Appendix 4 and a limit of liability of $100,000 in the RFT and draft contract. Additionally, the evaluation criteria in the RFT and the supplier obligations in the draft contract were drafted to emphasize the importance of the supplier's management of sub-contractors. 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 ingoing service delivery.

Case Study 3 – Installation of a Word Processing Application on Agency Network

Background

An Agency requires a new word processing application to be installed on its network. The required application is a proven, mature application which is known to work well with other applications on the network. The licences for the application will be purchased under a whole of government software agreement. The Agency is seeking a supplier to install the application. The Agency estimates that the cost of installation will be $60,000. The Agency will seek quotes from suppliers on its existing IT services provider panel.

Preliminary Risk Assessment and Preparation of Request for Quote

The procurement officer prepared a Context Statement (similar to the statement in Table 1) to assist the officer to identify key project objectives, stakeholders and evaluation criteria. The procurement officer's initial view is that the procurement is a simple procurement and low risk.

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

Given the Agency 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 was also considered to be low as the Agency intended to back up all data prior to installation. The brainstorming session estimated that recovering data from back up tapes and fixing poor installation could cost the Agency $10,000. The Agency sought a liability cap of the value of the contract.

Nonetheless, the procurement officer decided that the consequence of the risk eventuating were sufficiently significant to include provisions in the contract that required the supplier to perform specific acceptance tests.

The procurement officer cited and kept a copy of all insurances that the RFT and contract required the supplier to hold.

Case Study 4 - Development and roll-out of an Agency website portal, with capability to conduct a range of e-business and Government business functions.

Background

As part of an Agency's new approach to providing more on-line services, it has decided to implement a new website, including a portal to provide a range of services on-line to its customers. The Agency is seeking a supplier(s) to design, implement and maintain the new portal.

Preliminary Risk Assessment and Preparation of RFT

The procurement officer prepared a Context Statement (similar to the statement in Table 1) to assist the officer to 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 was most likely a borderline simple/complex procurement and medium risk; and
- the Agency will 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 at Table 2) by considering each key aspect of the scope of work.

The procurement officer had initially assessed the procurement to be a medium risk activity largely influenced by the few on-line 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" requested the procurement officer to expand the scope of work to increase the number of on-line 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, were of 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 the 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. The risks included:

1. failure or lack of availability of the portal may lead to Agency customers being unable to access information, or provide information, in the legislated timeframes;
2. sensitive business or personal information provided by agency customers through the portal may be lost or inadvertently passed to other agencies or organisations;
3. inaccurate information from the portal may cause the Agency to mislead its customers; and
4. Agency customers may 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 is quite moderate by comparison. Based on experiences elsewhere within the government, portal failure 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 that 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 may face. The model and analysis indicated that, with a 99.99% level of confidence, Agency liability for failures in the portal would not exceed $5m in total. As a result, the procurement officer stipulated a proposed limit of supplier liability of $5m in the RFT and draft contract.

The RFT included a contract based on GITC4, amended to include liability clauses similar to the provisions set out in Appendix 4. The RFT stated that respondents were to indicate compliance or otherwise with the clauses and required liability cap of $5m and specify any cost implications to the Agency of alternative liability caps (include the cost benefits of a lower cap(s)).

Evaluation of Tenders

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

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

The procurement officer cited and kept a copy of all insurances that the RFT and contract required the supplier to hold.

Ongoing Project Management

The Agency project owner continued to up date the register of risks, throughout the Project to ensure that identified risks were properly managed.

Case Study 5 - Development and implementation of a new, complex operational system, including software and hardware, for an Agency that links a number of different technologies and communication infrastructures

Background

An Agency has a requirement to develop a management system that integrates a range of systems and technologies into a single source of information and knowledge for use in highly critical, operational activities. The information that is to be integrated varies in complexity and maturity, and in the hardware used, and comes from a number of sources, internal and external to the Agency.

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 lengthy 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 at Table 2) by considering each key aspect of the scope of work.

The key conclusion reached from the risk assessment 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, as well as analyse the results before the RFT drafting is completed.

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 in operation 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 the risks included:

1. software and code may not be available for some of those older systems requiring integration;
2. companies may be reluctant to grant a license to access or modify code of existing systems to enable integration to occur, or they may charge excessive fees for the license;
3. development of new software or modification of existing off the shelf software to meet agency requirements may delay delivery of the system and/or increase costs;
4. changing Agency requirements on the functions and outputs of the new system may lead to delays and cost increases; and
5. failure of the system during critical operations may lead to significant losses to the Agency.

Input from stakeholders during the workshop confirmed with the procurement officer 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 licenses to obtain and modify existing software would be difficult to obtain and would frustrate the contract if they were not obtained. The probability that the new system may fail in operation was assessed as reasonably low, however.

Limit of Liability

The risk assessment concluded that the cost to the Agency in terms of operational failure resulting from the system failure was not significant in financial terms, although system failure would impact on national interests. The consequential loss that the government may 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 in the range of $20,000,000.

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 degree of confidence of 99.99% that the Agency may face financial impacts of up to $25,000,000 as a result of the stated risks occurring.

As a result, the procurement officer placed a limit of supplier liability of $25,000,000 in the RFT and draft contract. Additions to the draft contract also included specific requirements on guaranteeing access to software, code and licenses are reasonable and fully costed rates, and guaranteed availability and reliability levels of the system in operation. System back up and business continuity plans were also mandated in the contract.

Appendix 7 – Useful References

Websites

Standard Australia - **www.Standards.com.au**

Endorsed Supplier Agreements - **www.esa.finance.gov.au**

Commonwealth Procurement Guidelines through the DOFA website - http://www.finance.gov.au/

Documents

Standards Australia (2004), Australian/New Zealand Standard AS/NZS4360:2004 Risk Management, Standards Australia, ISBN 0 7337 2647 X

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

Appendix 8 - Qualitative Measures Of Consequence And Likelihood

Table 1: Consequence scales

Rating	Description
Severe	Would stop achievement of functional goals/objectives
Major	Would threaten functional objectives
Moderate	Necessitates significant adjustment to overall function
Minor	Would threaten an element of the function
Insignificant	Lower consequences

Table 2: Likelihood rating

Likelihood	Description
Almost certain	The event is expected to occur
Likely	There is a very high likelihood that this event will occur
Moderate	There is a high likelihood that this event will occur
Unlikely	There is a fair likelihood that this event will occur
Rare	This event is not expected to occur

Table 3: Risk priority matrix

Likelihood	Consequence				
	Insignificant	**Minor**	**Moderate**	**Major**	**Severe**
Almost Certain	Medium	Medium	High	High	Extreme
Likely	Medium	Medium	Medium	High	Extreme
Moderate	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Appendix 9 – 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 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. With this in mind, this Guide provides a list of typical risks that may impact on an ICT procurement.

Checklist of typical ICT Contract risks

Agency Risks

Description of Risk	
	Technical Risks
أ	Poor information provided by the Government during the tendering process leads to inaccuracies in tenders and the contract.
أ	Government furnished material and information is not provided as contracted, leading to the supplier being unable to provide services in the required timeframe.
أ	Government provided information proves to be inaccurate or unrealistic, leading to delays in the supplier delivering the contracted services
أ	The agency is unable to provide sufficient resources to manage the contract and supplier interface.
أ	The Contract Statement of Work may be poorly written and not accurately reflect the actual services to be provided or customer requirements. A specific example may be accurately defining the interfaces and responsibilities with other systems.
أ	Existing agency systems are not properly maintained leading to delays in the delivery of services by the supplier.
أ	Poor systems “house-keeping” by the agency, including unauthorised software and hardware installations, and poor asset management, may result in the supplier being unable to effectively undertake the contracted services.
أ	Activities associated with other ICT projects and day-to-day operations clash with priority supplier tasks, leading to schedule delays.
أ	Undocumented configuration changes in agency ICT systems may result in additional work by the supplier.
أ	Agency Test Environment is not adequate for supplier tests.
أ	Agency security and facility access regulations may cause the supplier difficulties in undertaking the contracted services.
أ	Agency organisational changes cause supplier difficulties and result in having to change contract requirements.
أ	Problem resolution between multiple agencies may cause difficulties for the supplier in delivering contracted services.

Description of Risk	
أ	Elements of the ICT infrastructure may be under the control of third parties and may influence the ability of the supplier to provide contracted services
أ	The supplier may be unable to access 3rd party software used by the agency on the system, leading to delays and frustration of the contract.
	Commercial Risks
أ	The agency organisation fails to adopt the new services or systems.
أ	Lack of communication within the agency about the supplier's activities and contract responsibilities may delay the supplier in undertaking the contracted services.
أ	Agency workforce may not fully cooperate with the supplier in the delivery of the services leading to delays.
أ	The agency lacks expert advice and guidance, leading the difficulties in the supplier delivering the services required.
أ	Agency corporate knowledge and key skills are lost or minimised as a result of the supplier undertaking the work.
أ	Agency business requirements change after the contract is signed and lead to difficulties with the supplier
أ	A lack of controls leads to undisciplined or unauthorised changes to contract scope or services.

Supplier Risks

Description of Risk	
	Technical Risks
أ	Complexity brought about by multiple systems interfaces cause service delivery failures
أ	Supplier integration of services with existing ICT systems or communications networks is difficult and causes delays or termination of the contract.
أ	The supplier may not use proven and current technology in the provision of its services.
أ	Supplier fails to allow for continuous improvement resulting in inability to meet contracted Service Levels
أ	The supplier is unable to improve its workforce skill levels through the life of the contract, leading to failure to achieve contracted Service Levels
أ	Mobility of agency workforce affects ability of the supplier to complete the contracted work.
أ	Poor reliability of new systems leads to failure to meet contracted Service Levels.
أ	The supplier is unable to maintain the necessary skill levels over the course of the contract, leading to a reduction in Service Levels.
أ	Staff turnover and loss of skills within the supplier workforce results in poor levels of service as the contract progresses

Description of Risk	
A	Supplier is unable to provide the infrastructure support or assets it promised in the contract, leading to delays and possible termination
A	Supplier is unable to access necessary technology required to undertake the contracted services.
A	Supplier cannot obtain necessary security clearances to provide the services required by the contract.
A	The services provided by the supplier are unable to meet the growth and flexibility requirements of the agency
A	Supplier is unable to provide services as per the contract due to unplanned changes in the agency ICT environment.
A	Failure of the supplier to obtain, or loss of, quality and other required accreditations leads to inability to complete the services as contracted.
A	Poor design of software and documentation by supplier leads to difficulties in through life support.
A	Supplier conducts unauthorised activities in agency ICT systems, leading to system problems, damage or failures.
A	Supplier may use inappropriate tools to deliver the services leading to poor service or physical damage to agency systems.
A	The supplier may introduce unauthorised software or technology to the agency system.
A	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.
A	The supplier may move or remove agency equipment or material, leading to loss of agencies assets.
A	The supplier may reduce the level of diligence in the care of agency materiel on the assumption that the agency will meet replacement or repair costs to lost or damaged material.
A	Sensitive information on agency networks may be accessed by the supplier, leading to breaches of confidentiality and privacy.
A	The supplier may misuse agency data for its own purposes.
A	Supplier may not recognise the priority to be afforded to critical services (medical, financial, security) leading to agency dissatisfaction, and possible termination
A	The supplier may refuse to release proprietary information or technical data to the agency that is necessary under the requirements of the contract leading to an inability of the agency to support the system into the future.
A	The supplier may cause unacceptable disruptions to Defence operations in the conduct of its work.

Description of Risk	
أ	The supplier may not have a disaster recovery plan for serious virus infections. On discovery of a virus infection, the supplier may not take immediate action to eradicate the virus, restore operational efficiency or recover lost data.
أ	Supplier products or systems may introduce bugs or viruses into the agency network.
أ	The supplier may not provide all information and assistance necessary to conduct disengagement as efficiently and effectively as possible.
	Commercial Risks
أ	Supplier is unable to recruit suitable staff to provide the services required under the contract.
أ	The supplier may disrupt agency services by actively seek to recruit key agency personnel during the early stages of the contract.
أ	Supplier is not adequately resourced to manage the workloads required by the contract.
أ	Services may be delayed or impacted by inappropriate or under-resourced supplier transition activities.
أ	Poor sub-contractor management or sub-contractor performance leads to inability of the supplier to meet contract requirements
أ	The supplier or one or more of its sub-contractors may have a legal arrangement with an entity that creates a conflict or perceived conflict of interest with the performance of the contract.
أ	The supplier may not comply with OH&S laws, or agency obligations and policies relating to OH&S.
أ	The supplier may become insolvent or cease or threaten to cease to carry out its business, and make an arrangement with or for the benefit of its creditors that would make the continuance of the contract unworkable.

Joint Risks

Description of Risk	
أ	The Agency and supplier experience a cultural clash leading to misunderstandings, disputes and a poor relationship.
أ	Criteria for acceptance of supplier services is not well understood or agreed prior to the acceptance activity, leading to disputes over the acceptance activity.
أ	The Agency and supplier are in disagreement over the measurement of service level performance during the course of the contract
أ	Lack of Disaster Recovery and Business Continuity Plans from Agency and supplier results in major loss of services in the event of a system failure.
أ	Supplier expectations of services and support may not align with agency's requirements for 24/7 operations, leading to contract disputation.

Description of Risk	
أ	Inadequate Agency performance benchmarks and reporting tools, or failure of the supplier to maintain adequate documentation or appropriate tools to manage the contract, may lead to ineffective performance measurement.

Appendix 10 – Example Risk Register

ID #	Risk Description	Controls	Consequence	Likelihood	Additional Risk Treatment	Responsible Officer
1	Supplier may use inexperienced staff who fail to follow correct procedures, 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 design features of the system	$75,000	1 in 1,000	Contract to include additional installation acceptance testing and check requirements	Engineering Manager
2	Supplier sub-contractors may be late in delivering materials and services, leading supplier to delays in meeting installation deadlines and additional costs of running old systems	Selection of well-proven sub-contractors. Detailed agreements with sub-contractors. Effective sub-contractor management processes	$25,000	1 in 100	Include requirement that Agency approve selection of sub-contractors	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 1,000	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
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 HR 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 may 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 1,000	Require extensive lab test and trials of new systems prior to acceptance and installation Improve data backup capabilities prior to installation of new system	Engineering Manager

9	Supplier staff may 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 1,000	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 to contract signature	Contracts manager
11	Agency and supplier disagree over the measurement of service level performance during the course of the contract, 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 prior to contract signature Do not impose unrealistic service levels.	Contracts Manager
12	The supplier may be unable to access 3rd 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 1,000	Add provisions to the contract that allow termination if access to 3rd party software cannot achieved in reasonable timeframe	Contracts Manager

Appendix 11 - Key Legislative Provisions and Policies Relevant to ICT Procurement

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

   - the *Financial Management and Accountability Act 1997* (**FMA Act**) (especially sections 5 and 44);
   - *Financial Management and Accountability Regulations 1997* (**FMA Regulations**) (especially regulations 3, 7, 8, 9, 10, 12 and 13); and
   - the Chief Executive Instructions (CEIs) for each Agency, issued under FMA Regulation 6, in accordance with section 52 of the FMA Act.

2. 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* (**CAC Act**) (especially sections 47 and 49),
   - *Commonwealth Authorities and Companies Act Regulations 1997* (**CAC Regulations**) (especially regulation 9) and
   - the Finance Minister's (CAC Act Procurement) Directions 2004.

Overview of policy framework

The Financial Management Guidance series of publications

No. 1 Commonwealth Procurement Guidelines, January 2005 (**http://www.finance.gov.au/ctc/commonwealth_procurement_guide.html**)

No. 2 Guidelines for the Management of Foreign Exchange Risk, November 2002.

No. 3 Guidance on Confidentiality of Suppliers' Commercial Information, February 2003.

No. 4 Commonwealth Cost Recovery Guidelines for Information and Regulatory Agencies, March 2003.

No. 5 Guidelines for Implementation of Administrative Arrangements Orders and Other Machinery of Government Changes, September 2003.

No. 6 Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort, September 2003.

No. 7 Guidelines for the Management of Special Accounts, October 2003.

No. 8 Guidance on the Listing of Contract Details on the Internet (Meeting the Senate Order on Department and Agency Contracts), January 2004.

No. 9 Australian Government Competitive Neutrality Guidelines for Managers, February 2004.

No. 10 Guidance on Complying with Legislation and Government Policy in Procurement, January 2005.

No. 11 The Role of the CFO – Guidance for Commonwealth Agencies, April 2003.

No. 12 Guidance on Identifying Consultancies for Annual Reporting Purposes, July 2004.

No. 13 Guidance on the Mandatory Procurement Procedures, January 2005.

Standards Association of Australia, Australian and New Zealand Standard, AS/NZS 4360:2004 *Risk Management,* 2004

Australian National Audit Office, *Contract Management: Better Practice Guide* available from **http://www.anao.gov.au**

Australian National Audit Office, *Selecting Suppliers - Managing the Risk* available from **http://www.anao.gov.au**

Department of Finance and Administration, Finance Circular 2003/02 *Guidelines for Issuing and Managing Indemnities, Guarantees, Warranties and Letters of Comfort* available from **http://www.finance.gov.au**

Department of Finance and Administration, Finance Circular 2004/05 *Financial Management and Accountability Regulation 12* available from **http://www.finance.gov.au**

Department of Finance and Administration, Finance Circular 2004/10 *Using the Financial Management and Accountability Regulation 10 Delegation* available from **http://www.finance.gov.au**

Management Advisory Board, MAB/MIAC Report No. 22 *Guidelines for Managing Risk in the Australian Public Service,* October 1996, for availability details contact **http://www.apsc.gov.au**

The ESA program is managed by the Department of Finance and Administration. More information on ESA is available at **http://www.esa.finance.gov.au**

18.16 The FMA Regs impose additional requirements:

18.17 Reg 8(2)- any official who takes an action that is not consistent with the CPGS must make a written record of his or her reasons for not doing so

- Reg 9 and 12- where approval of a proposal to spend public money is not given in writing, the approver must make a record of the terms of the approval in a document as soon as possible.

CPGs

http://www.finance.gov.au/ctc/commonwealth_procurement_guide.html

ENDNOTES

[i] E.g. hardware malfunction (faulty CRT monitor) starts fire and burns down Cth building.

[ii] Eg. physical security breaches could involve, or lead to, breaking and entering and could cause property damage.

[iii] Eg. MAC services improperly performed by technician, causing property damage in the course of the MAC.

[iv] Eg. drunk service provider personnel drives vehicle into Cth building.

[v] Examples of economic loss includes rent on damaged building, of productivity

[vi] Eg. hardware malfunction (eg faulty cable or CRT monitor) means Agency needs to rent new premises to work from and loss of productivity.

[vii] Eg. if the IP is not available as contracted (ie because 3rd party holds all the IP rights), cost of procurement of the withheld IP or alternative IP is an economic loss.

[viii] Eg. breach could result in loss of commercial value of the protected info and costs of investigation.

[ix] Eg. costs of investigation of breach might arise.

[x] Eg. failure to maintain server prevents Cth officers from working.

[xi] Eg. incorrect input of data requires re-input of data, fixing up flow-on effects of incorrectly entered data.

[xii] Eg, Hardware malfunction (eg faulty power supply/cable or CRT monitor) sets fire killing inhabitants or causing noxious fumes inhalation.

[xiii] Eg. hardware malfunction (eg faulty power supply/cable or CRT monitor) sets fire burning down landlord's building,

[xiv] Economic Loss not consequential on personal injury, death or property damage. Courts are reluctant to find a duty of care in such cases and therefore these damages are not commonly awarded.

[xv] Compare this approach to GITC4 which encourages damages arising from negligent acts or omissions to be unlimited.