Wigley & Company

BARRISTERS and SOLICITORS

Capping Liability the Australian Way

September 2006

The 64 thousand dollar question

"So what should the cap on liability be?" – A common question for all those that have been involved in drafting or negotiating an IT or telecommunications agreement. Getting to that magical figure can resemble more of an art than a science. More often than not the total liability of a supplier is determined by rules of thumb such as a figure that will help "keep the supplier honest" or just a multiple of the value of the contract.

It's not uncommon for a customer to shrug off an analysis of liability on the basis that "if we get to that stage the relationship's stuffed anyway" or "we're never going to sue". Of course, both statements may be true. However, they also ignore the significant costs of project failure and the incentive that an appropriate cap on liability can have in motivating a supplier to deal with problem projects.

In some cases a position is taken that requires that the supplier should have unlimited liability. Suppliers strongly object to such a stance. It is in this context that the Australian Government has recently released policy on limiting liability in information and communications technology contracts.[1]

The new Australian policy

The new policy provides that:

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

This approach reflects appropriate New Zealand practice, both in the public and private sectors. Some organisations start from the assumption that there shouldn't be limitation of liability at all. That is not realistic.

If a supplier is to have unlimited liability it may need to "gold plate" its products and services with risk premiums and insurance to address its potential exposure – a costly proposition. In other cases suppliers just won't pitch for the work because the risk is too great. When faced with the choice, most customers opt for a cap on liability in the interests of getting the solution they want, at an acceptable price.

That's not to say that customers don't push for unlimited liability when they think they have the leverage to succeed. In this respect the policy is a win for ICT businesses in Australia. Senator Helen Coonan, the Minister for Communications, Information Technology and the Arts, said:[2]

> "Introducing caps on ICT supplier liability is good for business, especially smaller businesses, as reducing the liability coverage required will decrease the costs of tendering and doing business with the Government".
>
> "These savings should also flow through to tendered prices, delivering better value for money for the Government and taxpayers."

Of particular interest is the accompanying Guide to the policy that sets out how agencies can determine the cap on liability.[3] The aim of the Guide is to assist agencies to implement the policy and to help suppliers understand how the policy will be implemented. A quick reference overview of the Guide is also available.[4]

Highlights from the policy and guide

Key points from the policy and Guide include the following:

---

[1] The policy can be read in the Finance Circular 2006/03 at www.finance.gov.au/finframework/fc_2006_03.html (also see Appendix 2 of the guide)

[2] www.minister.dcita.gov.au/media/media_releases/guide_to_limiting_supplier_liability_in_ict_contracts

[3] *A Guide to Limiting Supplier Liability in ICT Contracts with Australian Government Agencies* at www.dcita.gov.au/ict/procurement_and_industry_development/capping_suppliers_liability_in_ict_contracts

[4] Ibid.

- The Guide does not intend to mandate a "one size fits all" approach. Instead, it provides examples of how agencies may implement the policy. The approach will vary depending on how risky the ICT procurement is.
- The Guide suggests that a risk management and assessment process be undertaken. The Guide includes a process that builds upon the Australian/New Zealand Risk Management Standard AS/NZS4360:2004 and sets out the following five steps:[5]

  Establish the context of a risk assessment – includes analysis of the background of the project, its objectives and stakeholders.

  Risk identification – includes considering when, how and why risks might occur.

  Analysing the risks – includes evaluating the consequences and likelihood or each risk occurring (note that the guide suggests that consequences be quantified in dollar terms to assist with allocating liability and reaching a figure for the total cap).

  Evaluate the risks – do the risks need to be addressed, and in what priority?

  Treatment of the risks – identify the options and develop and implement plans for the preferred options (this goes beyond just setting an appropriate cap to taking steps to address the identified risks).
- Following completion of the risk assessment the next step is to estimate and allocate liability under the contract. Methods of estimating liability range from the basic (picking the highest value risk) to sophisticated (construction of risk models and use of specialised software).
- The notes accompanying the policy clarify that it is generally appropriate for there to be uncapped liability in relation to the following matters:
  - Personal injury (including sickness and death);
  - Unlawful or illegal acts;
  - Damage to tangible property;
  - Intellectual property obligations;
  - Confidentiality and privacy obligations; and
  - Security obligations.
- The Guide deals specifically with "shrinkwrap", "click wrap" and "web-wrap" agreements. Although such agreements can be unclear and provided to a customer on a "take it or leave it" basis the guide suggests they should still only be accepted if the supplier's cap on liability (or, as is often the case, exclusion of all liability) is appropriate in view of the risks faced by the agency.
- If a supplier wishes to exclude "indirect" or "consequential" losses the Guide recommends that agencies consider clarifying exactly what those losses are, check that the risk assessment support the supplier excluding such liability, and consider whether there is any justification from the supplier as to why such liability should be excluded if its total liability is capped.
- Consider other clauses in the agreement that may limit the supplier's liability. For example, clauses that limit performance or delivery obligations, exclusions from any warranties and the force majeure regime.
- Appendix 8 of the Guide includes a helpful checklist of typical ICT contract risks to consider. However, the Guide does not advocate a pure "check list" approach to addressing risk. Instead, it recommends brainstorming type activities to identify the risks and their consequences.

A cap of ten times the contract price?

Appendix 5 to the Guide contains five case studies to illustrate the application of the practices set out in the Guide. Of particular interest is Case Study 5 which relates to the development of a new, complex operational system, costing $2.5m. The agency's risk assessment concluded (with the help of models and simulations) that, with a degree of confidence of 99.99%, the agency may face financial impacts of up to $25m if the stated risks were to occur. Consequently, the cap was set at $25m.

This is a far cry from the standard supplier approach of capping liability to the amounts paid under the contract! Most suppliers would balk at the prospect of a cap on their liability being ten times the contract price. However, it

[5] Figure 4 in the companion to the guide sets out a helpful summary diagram.

is important for suppliers to recognise that the potential losses that the customer could incur if the supplier fails to deliver as promised will, in many cases, exceed the amounts paid to the supplier. Undertaking proper risk analysis will often reveal whether this is the case.

Too much hard work for just one figure?

Some may think that all this risk analysis is overkill in the interests of arriving at a dollar figure. However, there is significant value in the journey as well as the destination. While the cap on liability is most often relevant as the ambulance at the bottom of the cliff, a considered assessment of the risks associated with any ICT project is an essential step in avoiding project failure. The risks need to feed into appropriate governance, management, remedial and disputes structures and processes to avoid, and deal with, all those factors that could push a project off the rails.

While undertaking the type of risk assessment recommended by the Australian Government can be time intensive it is still good practice as it results in more appropriate allocation of risk and can increase the likelihood of project success.

We welcome your feedback on this article and any enquiries in relation to its contents. This article is intended to provide a summary of the material covered and does not constitute legal advice. We can provide specialist legal advice on the full range of matters contained in this article.
