proximity LEGAL

COMMONWEALTH ICT PROCUREMENT: TIPS AND TRICKS

THE PRESENTERS

James Dunn

James Dunn is a Director of Proximity Legal, an innovative secondment legal practice that offers clients the flexibility and varied experience of outside counsel combined with the commercial focus of in-house counsel. James has built a strong reputation in the Australian Government legal and procurement sector as a dependable, practical and outcome focused advisor. James' main areas of practice are government contracting and procurement. James has a particular focus on information technology and capital acquisition procurement, intellectual property and software licensing. He has played an important role in the provision of legal and procurement services to the Australian Government for a number of high profile and complex projects, including the establishment of whole-of–government ICT panels.

David Mahony

David is a Principal Advisor at Proximity Legal with particular experience in Australian defence contracting and procurement, intellectual property and technology, corporate governance and business ethics. Prior to joining Proximity Legal, David held senior legal positions with a leading global aerospace and defence company, including many years heading up the legal function of the company's Australian subsidiary whose principal customer was the Australian Department of Defence. David enjoys achieving effective and practical legal and business outcomes, paying close attention to detail while retaining the ability to see the strategic issues and realistically analyse and assess the appropriate action to achieve effective legal and business outcomes.

INTRODUCTION

ICT is becoming an increasingly important part of our personal lives and the operations of business and government. ICT is able to greatly improve an Agency's business and operational processes and the services it provides to the public. It can also assist with lowering an Agency's bottom line.

The Australian Government ICT Strategy 2012-2015 was launched by the Secretary David Tune in September 2012. The Strategy statement is:

> *"The APS will use ICT to increase public sector and national productivity by enabling the delivery of better government services for the Australian people, communities and business, improving the efficiency of APS operations and supporting open engagement to better inform decisions."*

ICT includes the procurement of more traditional forms, such as software and hardware, but also includes cloud computing and website services.

Many procurements undertaken by Agency's have an ICT component; even if the primary equipment or service is not ICT related (for example, ships for Defence or an asset management system for the ATO). It is therefore important that Agency procurement officials have a strong understanding of the key risks and issues relevant the procurement of ICT.

This paper is practical in nature with few references to legal cases or legislation. The intention is to provide a basic overview of how to procure key forms of ICT goods and services and highlight some of the lesser known risks that need to be managed when negotiating contracts with ICT suppliers.

While the presentation has a particular focus on the procurement of hardware and software, the protections and principles covered in this paper can be applied to other types of ICT procurement.

OVERVIEW OF THE COMMONWEALTH ICT PROCUREMENT FRAMEWORK

Changing procurement landscape

The last five years have seen significant changes in the way the Commonwealth procures ICT goods and services. The current Government's program to reduce the operational expenditure of Commonwealth Agencies has largely focused on ICT goods and services because many of these services can be commoditised and are common across Agencies. The Australian Government has introduced whole-of-government (WoG) ICT panels and implemented other recommendations from the review into the Australian Government's use of ICT conducted by Sir Peter Gershon in 2008[1].

Proximity Legal has been involved in a number of engagements recently to assist agencies to both establish and use WoG ICT procurement arrangements.

AGIMO reference material

The Australian Government Information Management Office (**AGIMO**) website provides a really good overview of the key legislative and policy requirements for conducting ICT procurement in the Commonwealth. These requirements include the following[2]:

- Policies and standards (including for cloud computing, open source software, data centres etc)
- Guides and checklists (including in relation to e-procurement, managing websites etc)
- Templates and contracting frameworks (e.g. SourceIT model contracts and general Commonwealth procurement rules and guidelines that apply to ICT procurement)
- Mandatory and voluntary WoG panels (e.g. Desktop Hardware Panel and telecommunications panels).

Commonwealth procurement personnel and lawyers and other external providers who assist the Commonwealth with procurement will find these materials very useful and they assist to simplify what can sometimes appear to be a complex procurement framework.

[1] http://www.finance.gov.au/publications/ict-review/docs/Review-of-the-Australian-Governments-Use-of-Information-and-Communication-Technology.pdf

[2] http://agimo.gov.au/policy-guides-procurement/

ICT specific policies and panels

The key policies and guidance documents that apply specifically to ICT procurement are on the AGIMO website. These include policies that prescribe when and how the Commonwealth's ICT panels and other arrangements must be used.

One of the key guidance documents that applies specifically to ICT procurement is the 'Guide to limiting supplier liability in ICT contracts with Australian Government Agencies'[3]. The guidance reflects an understanding that requiring unlimited liability (and inappropriately high levels of insurance) can impede companies in providing ICT to Agencies[4]. Unlike non-ICT procurement, the default approach in ICT contracts is to limit a supplier's liability unless there is a compelling reason otherwise. The guide provides really useful instruction on how to develop and implement risk assessments and risk treatment strategies.

Some of the key WoG panels and other arrangements that are either mandatory or available for Commonwealth Agencies to use are the:

- Data Centre Panels and Data Centre as a Service Multi-Use List
- Desktop Hardware Panel
- Gatekeeper PKI Service Provider Panels
- ICT Management Consultant Multi Use List
- ICT Multi Use List
- Microsoft Volume Sourcing
- Portfolio Panels for IT Services
- Telecommunications Panels. See also the Australian Government Telecommunications Arrangement
- Internet Based Network Connection Services Panel
- Telecommunications Management Panel
- Telecommunications Commodities, Carriage and Associated Services
- Telecommunications Invoice Reconciliation Services

It is important that procurement officials consider whether their procurement falls within the scope of one of these arrangements before conducting the procurement. It is important to remember that these arrangements can apply differently to FMA Act Agencies and CAC Act Agencies.

[3] http://www.innovation.gov.au/Industry/InformationandCommunicationsTechnologies/Documents/LimitingLiabilityReport.pdf

[4] Page 1, http://www.innovation.gov.au/Industry/InformationandCommunicationsTechnologies/Documents/LimitingLiabilityReport.pdf

The changes to the Australian Government ICT procurement landscape, particularly the WoG ICT panel arrangements, have resulted in savings and streamlined the process for purchasing some types of goods and services. However, some ICT procurements will require the use of multiple WoG panels and other arrangements and this can create complex procurement challenges. Integrating services procured from multiple panels, and establishing mechanisms to ensure clear lines of responsibility between different service providers, can be challenging.

WHAT IS DIFFERENT ABOUT ICT PROCUREMENT?

In one sense, ICT procurement is the same as any other Government procurement in that it must be carried out in accordance with the procurement framework set by legislation, regulations and policies, including compliance with:

- the *Commonwealth Procurement Rules* (CPRs), including the *Additional Rules* of the CPRs, for procurements over the relevant procurement threshold
- the *Financial Management and Accountability Act 1997* (Cth) and associated regulations for Agencies subject to the FMA Act, and
- the *Commonwealth Companies and Authorities Act 1997* (Cth) for entities subject to the CAC Act.

However there are a number of particular characteristics of ICT procurement:

1. Intellectual Property: ICT procurement is inherently ‘software rich’ and requires a good understanding of the legal risks and other implications, such as licensing, modifications and enhancements, maintenance and upgrades, and source code escrow, to ensure that the customer contracts for and acquires what it needs.

2. Technical complexity – the subject matter can be inherently complex and may not be well understood by non-ICT managers, and this is exacerbated by the continual and rapid evolution of hardware and software technologies.

3. Risk – understanding the enterprise’s existing and future business needs and matching them to the right technology solution is not a simple task. Data loss is a key risk that needs to be managed effectively by Agencies when procuring and using ICT goods and services.

4. Cost – ICT procurement is one of the more costly elements of procurement, across private industry as well as government and the public sector.

As a result, other than for simple out-of-the-box or shrink-wrap transactions, the use of the term ‘procurement’ can be slightly misleading as many ICT procurements are complex infrastructure projects and have to be managed in the same way as any major project. This entails factors such as:

- Detailed advance planning of the lifecycle process through requirements definition, solicitation, evaluation, negotiation, contract award, set to work, project delivery and project close-out

- Involved management and governance at different levels, including at senior executive level

- Clear lines of accountability and responsibility (with authority) for project delivery

- Detailed understanding of the scope of work, and careful management of scope change

- Good estimating and pricing – including a proper assessment of the customer’s resources that are going to be required to implement the project

- Realistic assessment of schedule and delivery dates

- Effective performance monitoring and active performance management

- Clear identification of key deliverables and the associated ‘gates’ for moving from one phase to the next

- Critical assessment of the supplier’s ability to deliver over the life of the project.

KEY TERMS FOR SOFTWARE CONTRACTS

What templates and terms to use

The value and complexity of software purchased or leased by the Commonwealth varies significantly. It is therefore important to determine what contractual terms are appropriate for the procurement. Some of the factors that will influence the template or other terms you adopt include:

- Whether the software is commercial-off-the-shelf (COTS) software, COTS software that requires modification, or new software that needs to be developed by the service provider (bespoke software);
- If the software is bespoke software, whether you want to own the software or receive a broad licence to the software
- Whether you require upgrades, updates, bug fixes and/or technical support for the software
- Whether you require extensive modification and adaptation rights
- Whether the software includes a high number of components owned by other third parties
- Whether the software will be integrated with other software and systems or has complex installation requirements.

The Australian Government's SourceIT template suite has the following two software procurement templates:

- COTS licence only
- COTS licence and support contract

One of these templates may be suitable for your procurement if your purchase is simple and does not require any software development or complex licensing, installation, support and maintenance arrangements. The SourceIT website provides guidance on when the templates should and shouldn't be used[5]. While the model contracts do not necessarily

[5] http://agimo.gov.au/policy-guides-procurement/sourceit-model-contracts/

remove the need for professional legal or procurement advice altogether, it should make the preliminary stages of agreeing terms for simple software purchases more efficient.

Licence rights

Standard Licence terms

The licence rights to the software that your Agency requires will depend on a range of factors including:

- how the business area or other Agency personnel will use the software;
- who needs access to the software (e.g. contractors that provide services integrated with the software or an Agency's outsourced provider);
- the platforms on which you will install the software (e.g. on a server or on individual desktops etc);

The licence may be:

- Perpetual - i.e. there is no end date for when the customer needs to stop using the licence. However, if the customer only requires use of the software for a specific period of time, the Agency should consider getting an annual subscription licence as this may be more cost effective
- Irrevocable – i.e. the supplier cannot revoke the licence rights during the period of the licence (unless the supplier has a separate right to terminate the licence)
- world-wide – i.e. the customer can use and access the software anywhere in the world. This is especially important for Agencies that have personnel working overseas (like DIAC, Customs and Border Protection, AusAID, Defence etc) and need to access the software.
- non-exclusive – i.e. the customer does not have an exclusive right to use the software because the supplier licences the software to other clients. This is a right that protects the supplier but has become a standard term in licences because the Commonwealth very rarely will require an exclusive licence to software
- royalty-free – i.e. the customer is not required to make any royalty payments for use of the software as the purchase price (or ongoing fees) for the software is full consideration for use of the software

A standard licence (like the one included in the SourceIT template) should allow the customer to install, adapt, modify (at least modify to enable use on the Customer's existing system), use and communicate each part of the Software and the Documentation in either hardcopy or soft copy and make copies of the software for back-up and security purposes. Agencies should not accept terms more restrictive than these unless there is a clear business reason for doing so.

In the context of Australian Government procurement, it is also important to ensure that your Agency has the right to assign its licence rights to another Agency that requires the software as a result of an Administrative Arrangements Order and has the right to sublicense to a third party if that third party is assisting the Commonwealth (e.g. third party contractors that assist the Agency and that require access to the software).

Pricing/licensing models

It is critical to determine the basis on which the number of licences is determined. This may have a significant impact on the price and may result in a customer breach if the customer does not comply with the contracted licence terms. Software can be licensed on a number of bases including:

- Per user based licensing – total users, names users or concurrent users
- Per desktop (or seat) licensing
- Enterprise licensing (e.g. a whole Agency)
- Per server licensing

Concurrent use licences allow an infinite number of users to access the software provided the number of users accessing the software at any one time does not exceed the agreed licence numbers. For example, an Agency could have 200 licences for an HR management system. The Agency could allow 600 users to use the HR management system provided there are processes in place that ensure no more than 200 are using the system at any one time.

If user based licensing is adopted, it is important to determine what a ‘user’ is. Does a user include contractors? Are users only FTE personnel or all personnel who might access the software? It is critical that Agencies have a strong understanding of the licence terms they require and comply with those terms.

For named user licences it is important to have a pre-determined process that will be followed if an named user no longer requires access to the software (eg if a named user has retired from their role and will be replaced by a new recruit).

Additional licence terms and protections

Agencies may require additional or alternative licence terms in order to manage particular risks or achieve broader rights to the software. Agencies should consider whether they require the right to:

- Customise and configure the software
- Transfer the software between the Agency's systems at no additional cost
- Make copies of the software for user training purposes
- Maintain and support the software if the supplier breaches its support obligations
- Re-install software without affecting the software warranties
- Deploy the software and documentation to servers or desktops through the use of virtualisation technologies

If the supplier is providing software that contains software sub-components that are owned by a different entity to the software supplier, try to secure the same licence terms for all the software or ensure that the supplier offers minimum standard terms for the third party component.

Some software suppliers will bundle and unbundle their standard software options during the term of the licence. For example, the supplier may sell you software A and then later bundle software A with software B to create software C. The supplier may then seek to charge the customer for the new and improved product. It is important to ensure the software licence in the contract applies to any bundled, rebundled, or rebranded software without any additional charges being payable by the customer.

Similarly, if the supplier removes functionality from the existing software as part of a rebundling of the software or the sale of that functionality to another software company, the contract should include an obligation for the supplier to provide that removed functionality at no additional charge and on the same licence terms.

Restrictions

It is common for software suppliers to include some restrictions in their licence terms. Whether certain restrictions are acceptable will of course depend on the Agency's requirements but some common restrictions that are generally acceptable include:

- No decompiling, disassembling or reverse engineering or otherwise trying to derive the source code from the object code
- No selling, renting, leasing, timesharing, transferring or sublicensing (unless otherwise authorised under the licence)
- a requirement for the Agency to ensure its personnel comply with the software terms (this will require personnel to be well trained).

Software Development

If an Agency requires a supplier to develop new software or modify the supplier's existing software, the Agency should consider including a number of additional protections, for example:

- a requirement for all intellectual property rights in the developed software to be owned by the Commonwealth (or a very broad licence to that developed software)
- a requirement that the source code, documentation and all other material needed to support the software are held with an independent escrow agent to ensure the customer can access this material in certain circumstances (see below for more details about escrow)
- a software engineering and development process with clear and detailed Acceptance Criteria and rigorous Acceptance Testing to establish compliance with the Acceptance Criteria

It is critical that Agencies consider whether developed software will be owned by the Agency or owned by the contractor. The Agency should conduct an 'IP Needs Analysis' to determine the Agency's preferred position with respect to the IP rights in the software. This is determined by working out what the Agency's needs are in relation to the software. Some considerations include:

- Is the software highly sensitive and use of the software by another party could impact national security (this may indicate that the software should be owned by the Commonwealth)
- Could the Agency, Commonwealth or marketplace benefit from the supplier owning the software and commercialising it (e.g. increasing the supplier's client basis may drive efficiencies for the supplier which reduce future licensing and support costs for the supplier's clients or result in increased product development and support)

- Could the commercialisation of the software by the supplier improve innovation in a particular market?
- Does the Agency have a need to commercialise the software (it is unlikely that it will unless commercialisation is part of the Agency's business (e.g. CSIRO)
- If the Agency does seek to own modifications that it has paid a supplier to make to the supplier's software, are the new software elements separately useable by the Agency. If not, there is little benefit in the Agency owning the modifications

If an Agency agrees to the supplier owning software developed for the Agency, the Agency should consider seeking a price discount that reflects the benefits the supplier is obtaining through ownership (i.e. the ability to commercialise a product for which the Agency has paid the supplier to develop). Agencies should not act as 'R&D' financiers.

The Australian Government Intellectual Property Manual[6] provides very useful guidance on how to conduct an IP Needs Analysis and how to determine whether the Agency should own or licence software developed for the Agency.

Escrow

For particular some types of software (e.g. business critical software on which a major system or asset is dependant), an agency should consider requiring the source code of the software to be held in escrow if the supplier will not agree to provide source code as a deliverable.

When including an escrow requirement, it is important to be clear about the escrow process including:

- When the supplier has to deposit source code in escrow (e.g. at incremental stages of the software development process or just upon final Acceptance of the developed software)
- How often the supplier is required to update the source materials in escrow
- The events that trigger a requirement for the escrow agent to release the source materials (e.g. expiration or termination of the software development contract or if the supplier fails to comply with its software support obligations)
- Which party pays for the cost of escrow (e.g. the costs are split between the customer and supplier or just the supplier)

[6] http://www.ag.gov.au/RightsAndProtections/IntellectualProperty/Documents/IntellectualPropertyManual.pdf

Technical Data

It is important to ensure the supplier has an obligation to provide documentation (including technical manuals) required by the Agency to properly exercise its rights to the software. This should include documentation that a software supplier would normally make available to its customers free of charge. The requirements for the documentation should be clearly set out including requirements for the documentation to be current and accurate and to be provided at no additional cost.

Support

If your Agency requires support and maintenance for the software you will need to consider the specific support requirements and some of the risks. These considerations include:

- Ensuring the payments for support and maintenance do not commence until after the software has been formally accepted
- Do you need updates? (e.g. bug fixes and changes that are made to overcome defects)?
- Do you need new releases (a substantially enhanced version of the software with new and improved functionality)
- Do you want the right not to take up new releases if you do not need or want the new software (e.g. because the Agency won't have time to test and integrate the new software into Agency's environment or it will interrupt another system upgrade)
- What service levels will there be for the support services (e.g. minimum telephone response times and resolution times for fixes, defect reporting timeframes, maximum number of outstanding defects etc)

It is important to ensure a supplier does not charge your Agency for services it is obligated to provide under its warranty obligations. For example, defects appearing in the warranty period are covered by the warranty component of the licence costs, not the support and maintenance costs. Ideally, the first year of support should cost less than later years as some of the 'maintenance' during this period could be warranty work.

Negotiating with large software suppliers

It may not be possible to secure some of the protections outlined above when negotiating with large software suppliers, particularly for very low value or complexity software arrangement. You should at least consider the need for these protections (and other protections included in more customer favourable government software purchase contracts). However, in some circumstances the protections may not be necessary or it may not represent value for money to seek to negotiate broader protections.

In higher value or more complex software procurements, it is possible to negotiate the inclusion of these protections in software licenses with some of the world's biggest software giants. In the last 5 years or so, more 'customer favourable' terms have been achieved with suppliers such as SAP, Microsoft and IBM on large deals and WoG arrangements.

It is worth liaising with other Agencies who have had recent experience procuring software from large suppliers to see if piggy-back options are available and to discuss additional protections the Agency has achieved, subject to the confidentiality restrictions in their software contracts.

KEY TERMS FOR HARDWARE CONTRACTS

Some people in the ICT procurement sector may consider software procurement as being more complex than hardware procurement. To some extent this view is true as software licensing can include more complicated IP elements and development work and the legal risks associated with software are constantly evolving. There are, however, many risks and issues that need to be considered and managed when procuring hardware. The successful integration of hardware and software in complex ICT systems is also a risk that needs to be closely managed. Below are some of the key risks and issues that should be considered when procuring hardware.

What templates and terms to use

ICT hardware can include desktop computers, laptops, servers, and mobile phones. The value and complexity of ICT hardware purchased or leased by the Commonwealth can vary significantly. It is therefore important to determine what contractual terms are appropriate for the procurement. Some of the factors that will influence the template or other terms you adopt include:

- Whether the hardware will be purchased or leased
- Whether there is software purchased with the hardware
- Whether there are complex installation requirements
- Whether you require support and maintenance for the hardware
- Whether the hardware will be installed at an Agency site, the supplier's site or a third party site (such as a data centre)

The SourceIT template suite has a hardware acquisition and maintenance model contract. This template may be suitable for your procurement if your purchase is simple, involves the procurement (not lease) of hardware, does not include the purchase of software through the same contract and is not complicated or multi-faceted (e.g. significant systems integration work is required). The SourceIT website provides guidance on when the template should and shouldn't be used [7].

Standard terms

Supply, delivery and installation

Some common requirements that Agencies should consider include:

- an obligation for the supplier to supply and deliver to the Agency the hardware specified in the Statement of Work.
- an obligation for the hardware to be newly manufactured, free from defects in workmanship and materials and comply with the manufacturer's specifications

[7] http://agimo.gov.au/policy-guides-procurement/sourceit-model-contracts/sourceit-hardware/

- details of the address to which the hardware must be delivered
- requirements for the preparation of the hardware prior to delivery (e.g. recording the serial number and asset number on the delivery docket, asset tagging the hardware, ensuring appropriate packaging material etc)
- requirements for the installation (including physical inspection of the hardware, connecting and configuring the hardware, ensuring the hardware is free of hazards etc)

Many hardware suppliers will require customers to 'Accept' the hardware on delivery, particularly in lease arrangements. It is important to include a requirement for the hardware to be tested prior to acceptance and payment as it is a lot easier for the customer to reject an item of hardware than it is to exercise rights of defect fix under a warranty. Agencies should consider including a requirement for the supplier to continuously operate the hardware for a period of time (e.g. 24 hours) and perform power ups and downs so the hardware reaches normal operating temperature before the Agency accepts the hardware.

Title to hardware and transfer of risk

It is important to ensure that title in the hardware does not transfer to the Agency until the Agency has accepted the hardware. This is important for a number of reasons including:

- Agencies should not accept hardware that is not working
- Agencies should not pay for hardware unless it has been accepted
- Suppliers will not want to transfer title until payment is received

The contract should also include warranties from the supplier that it has the required title, power and authority to supply the hardware to the customer.

Typically risk transfers with the physical item. Therefore, if an item of hardware is delivered to an Agency for testing, risk for loss or damage of the item will transfer at the time of delivery (even though title has not transferred because acceptance will not take place until after successful completion of acceptance testing). However, if the supplier is installing the hardware and is conducting the testing, it may be appropriate for the supplier to retain risk for loss or damage until it has completed these activities.

Third party warranties

Agencies should include an obligation in the contract for the supplier to ensure the customer receives the benefit of any standard third party or manufacturer warranties that apply to the hardware (e.g. if the hardware has multiple sub-components, the standard manufacturer warranty applying to all the sub-components). The contract should make it clear that this obligation does not limit the warranties that the supplier provides directly to the customer (e.g. the warranty that the hardware will comply with the specifications agreed between the parties).

Embedded software

If there is software or firmware (including operating system software) that is installed or provided on the hardware, the contract should include, at a minimum, an obligation for the supplier to grant the Agency a licence to use that software. The licence should allow the Agency to use the hardware for the purposes outlined in the contract. If the contract also separately covers the license of software and that licence provides more extensive rights (as outlined in the software section of this paper), the Agency should seek to include an obligation for the software contained on the hardware to be subject to the terms of that more extensive licence.

Import and export approvals

As a lot of hardware is manufactured overseas, it is important to include provisions that obligate the supplier to secure all the necessary import and export licences or other approvals needed to meet the requirements of the contract. It is important that the contract clearly states these requirements are included within the contract price. The contract should also include an obligation for the supplier to inform the Agency if any licence or approval is revoked or qualified or if new licence or approval requirements emerge during the term of the contract.

Support requirements

If your Agency requires support for the hardware, you should clearly document these requirements in the contract. Support services may include:

- a requirement to ensure replacement parts are available for a minimum period of time (e.g. the useful life of the hardware)
- a requirement that faulty parts are not removed from the Agency's premises (or an obligation to ensure that all defective hardware is erased of any software or other data relating to the Agency)
- an engineering change service or upgrade requirements (including a right for the Agency not to accept an upgrade)
- a service desk requirement and performance requirements for that service desk including minimum call pick up times, defect resolution times, defect reporting times etc

As with software, Agencies should ensure they do not pay for fixes during the warranty period.

KEY ISSUES FOR COMPLEX ICT SERVICE CONTRACTS

What templates and terms to use

The SourceIT model consultancy contract is a basic consultancy services template for the provision of professional services e.g. preparation of report/specifications, assistance with procurement process, or provision of training.

It is not suitable for more complex procurements of ICT consultancy services, for example ones with developmental aspects or for managed services. These will be done by way of bespoke contracts which may draw on or contain provisions similar to SourceIT model contracts such as the software licence and support contract and the old GITC v4.1 framework.

Notwithstanding the absence of Australian Government templates for complex ICT services and outsourcing contracts, there are nevertheless a number of key issues that are distinctive to complex service contracts which are discussed below. This section focuses on just a few of the key project and management issues that need to be considered in complex service and outsourcing arrangements.

Manage project delivery

Resist any 'just leave it to me' attitude on the part of the service provider and maintain effective operational control of the project by including in the contract:

- sufficiently detailed performance criteria and assessment measures; and
- details of when progress or review meetings will be held and the nature and timing of any reports or documentation to be provided.

Build in and use operational controls to support contract management. Involve the customer management team in setting up the process, as well as the supplier's service delivery team, to ensure that the process reflects the way they are going to operate.

Use the various elements of the process (reports, meetings, gates/review points, management escalation) proactively. There is little point having them if the customer does not understand and manage to the contract and enforce its provisions where necessary.

For example:

- only sign-off on acceptance or delivery of any phase when all documentation, including any reports, have been properly considered, reviewed and finalised;
- any corrective actions should be clearly identified and either rectified before agreeing to move on, or allowed as concession for rectification within an agreed schedule (with consequences for non-performance such as withholding of payments)
- through the process pay attention to and act on any warning signs or anything that rings an alarm bell - prevention or early action is much more effective than a later cure or letting a problem fester, particularly with the benefit of hindsight.

Maintain contractual control

Any government contract will have provisions giving the customer control over anything that amounts to a contractual change, including change to the scope of the services.

In service contracts, however, the service provider is encouraged (and expected) to find and share efficiencies and innovative practices in the delivery of the services as they evolve and mature.

The customer might derive less value from a service contract if it is unduly prescriptive about required service inputs and is resistant to changing its own practices in order to accommodate service provider innovation. Nevertheless, the customer still needs to balance the appropriate level of assurance to satisfy its regulatory and policy requirements and to assess the risk of any business impact from any change to the service.

Manage consequences of inadequate performance

In addition to including performance measuring and reporting requirements, so that graduated incentives and escalating deterrents can be applied progressively if contract performance falls below expected levels, complex service contracts also contain the full suite of customer protections for unsatisfactory performance:

- dispute resolution procedures with escalating levels of management involvement before mediation or arbitration, with litigation as a last resort;
- the right to give the service provider directions;
- the right to suspend the performance of work under the contract;
- the right for the customer to step-in and perform (or have performed) the work under the contract upon the occurrence of a specified event;
- the right to terminate, for default or convenience.

Always ensure that legal advice is taken on the options available under the contract at any stage to ensure that management decisions on next steps are better informed.

It can be tempting to consider termination for default if the other party is not performing to expectations, and it is particularly important always to obtain legal advice in these circumstances as wrongful termination can significantly adversely affect the terminating party.

In addition, although comprehensive termination clauses are essential they may be of limited practical use in isolation. Termination of the contract might leave the agency with no IT support in a critical business area unless another contractor can be found to take over a possibly unfamiliar system with no interruption in service.

Accordingly a transition-out or disengagement plan should be included to maintain business continuity while the services are being re-contracted. The GITC framework v4.1 contains an example at clause 6.4. The plan should provide for:

- novation or assignment of software licences and any relevant third party agreements
- transfer of any assets or equipment used in the provision of the services, and at what price (e.g. net book value, written down value, fair market value)
- transfer of data and material produced by the service provider in connection with the contract;
- knowledge transfer to key Agency personnel;
- co-operation by designated service provider personnel, with both the customer and any incoming or other supplier, for a specified period of time.

These disengagement services will inevitably come at a cost, and the customer should endeavour to have as much transparency about this as possible. It is preferable to have the cost for basic disengagement services (e.g. knowledge transfer, disengagement planning services etc) agreed at the commencement of the contract and then clear pricing metrics in the contract for determining more advanced and specific disengagement services.

Beware of a fixed termination fee which may seek to recover profit foregone by early termination, or unamortised costs. At the very least, a termination fee should decrease pro rata to the decreasing period of the contract.

Finally, endeavour to retain sufficient internal customer knowledge through continuity of personnel, and by on-going knowledge transfer during the contract period for example by requiring a detailed and regularly up-dated procedures manual.

PROCURING CLOUD SERVICES: STORM CLOUDS OR SILVER LINING

What is the Cloud?

Cloud Computing or Cloud Services refers to the access over the internet to business software and user data stored on servers at a remote location or locations. The term, and the technology concept, is not new. John Sheridan, Australian Government Chief Technology Officer (AGCTO), in his recent speech 'Seeding the Clouds'[8] specifically said 'There isn't any particular magic in the technology', and instead referred to it as 'a different way of buying IT services'.

The technology developments represented by the recent proliferation of lightweight portable devices with web browsers, and myriad associated operating systems, web user interfaces and software applications have facilitated on-line storage and hosting of data by third parties but do not represent a fundamental change to the concept of ICT.

AGIMO has developed very useful guidance material[9] to assist Agencies with procuring cloud services including guidance relating to:

- implementing cloud services
- privacy and cloud computing
- legal issues in cloud computing agreements
- financial considerations for using cloud services

Characteristics and benefits of Cloud Computing

Some of the characteristics of Cloud Computing are:

- Agility – technology infrastructure is quickly available
- Device and location independence – access from anywhere
- Maintenance – installation of computing applications is easier
- On-demand self-service – users can unilaterally obtain and deploy resources
- Reliability – improved if multiple redundant sites are used
- Scalability and elasticity - no need for users to engineer for peak loads

[8] http://www.cio.com.au/article/459136/inside_government_data_centre_transformation/
[9] http://agimo.gov.au/policy-guides-procurement/cloud/

- Virtualisation – increased utilisation by running several operating systems on a single Central Processing Unit (CPU)

Cloud computing should therefore result in lower costs and increased efficiency and flexibility in ICT Procurement.

Service Models

Cloud Computing services are typically offered in several fundamental models.

The most relevant for current purposes is 'Software as a Service' (SaS) – Cloud providers install and operate application software, and Cloud users access the software, over a network. Cloud users do not manage the Cloud infrastructure and platform where the application runs. This model simplifies maintenance and support.

Other Service Models are:

- Infrastructure as a Service – the Cloud provider offers access to additional resources such as data storage over a network to complement the user's local infrastructure.
- Platform as a Service – the Cloud provider delivers a computing platform (which could include operating system, programming language execution environment, database and web server) over a network and the Cloud user does not have to acquire and manage the underlying hardware and software.

Commonwealth Procurement of Cloud Computing Services

Much like the procurement of other ICT services, an agency will need to comply with the usual Commonwealth procurement legislation and policy.

The *Data Centre as a Service Multi Use List* established in October 2012 provides agencies with a simple way to procure Cloud services under contracts up to $80,000 (inclusive of GST) over a term of up to 12 months.

Issues in Cloud Computing

The benefits of cloud computing are numerous. However, there are a number of risks and threats that users, particularly Commonwealth Government users, should be aware of.

Commonwealth procurement officials should ensure that the key risks are managed through the procurement and contract drafting process. Some of these key risks are set out below.

- **Privacy**

  As with several of the following issues, this raises issues at both Australian and trans-border levels.

  Privacy and data security considerations must be addressed when transferring any personal information into a Cloud environment, and appropriate indirect controls put in place. See the OAIC *Better Practice Guide – Privacy and Cloud Computing for Australian Government Agencies*[10].

  If services are to be provided from outside Australia, particular care must be taken to put in place enforceable provisions that protect personal information. Agencies should identify the countries in which data will be stored and ensure they comply with the obligations in the *Privacy Act 1988* (Cth) relevant to the transfer of data overseas.

  Agencies should maintain control over use and sharing of information through effective contractual protections. At the very least Commonwealth Agencies must discharge their responsibilities under section 95B of the *Privacy Act* 1988 to take contractual measures to ensure that service providers do not breach the privacy principles. The service provider should be required (even if offshore) to comply with the *Privacy Act*, and the contract should contain specific provisions such as:

  - requiring the service provider to comply with principles regarding collection, use and disclosure of personal information;
  - ensuring the agency has the right to access, recover and correct personal information at all times;
  - restricting the flow of data off-shore; and
  - providing for how the information is dealt with at the end of the contract.

  Some service providers may have data centres in multiple and undisclosed locations, giving jurisdictional uncertainty. The customer can seek to specify in the contract the region or regions where the data will be stored and accessible, or where the data services centre will reside.

[10] http://agimo.govspace.gov.au/files/2012/02/Cloud-Privacy-Better-Practice-Guide-FINAL.pdf

- **FOI Compliance**

  Any Cloud services arrangements must permit the relevant agency to comply with its obligations under the *Freedom of Information Act 1982 (Cth)*, in particular accessing information in the event that an FOI request is received.

  In relation to compliance with Australian laws and regulatory requirements generally, be aware that information may be stored or processed through the Cloud in places with significantly different jurisdictional risks.

- **Security**

  Foreign government rights of access to data will apply in many overseas jurisdictions. It is important that Agencies understand which foreign laws apply to their data and assess the appropriateness of these laws. If an Agency is comfortable with a particular foreign government accessing the data in accordance with foreign laws, the contract should restrict such disclosure of data to circumstances where the disclosure is needed to meet an enforceable governmental request. The contract should require the service provider to notify the customer if data has been disclosed – and to notify the customer in advance of any disclosure, if permitted by law.

  The Privacy Amendment Act, and the Australian Privacy Principles which come into effect in March 2014, will impose more onerous requirements in relation to cross-border data flows in particular regarding notification to and consent from individuals. Agencies should ensure their contracts reflect these new requirements.

  See generally the AGIMO Better Practice Guide on this subject[11].

  Data security for cloud customers is a business risk as well as a legal risk (Privacy, FOI etc). Some typical data security issues, and the types of physical, technology or procedural controls that can be applied under customer contracts in order to maintain data security, are as follows:

  To protect data from unauthorised access by a third party:

  - Data encryption
  - Monitoring and management – by Agency & service provider
  - Gateway technologies

[11] http://agimo.gov.au/files/2012/04/privacy_and_cloud_computing_for_australian_government_agencies.pdf

- Email content filtering
- User authentication
- Service provider's security posture – physical & IT

To protect data from unauthorised access by other customers:

- Customer segregation
- Dedicated servers
- Media sanitisation

To protect data from access by unauthorised employees:

- Data encryption key management
- Vetting
- Agency or service provider auditing
- Restrictions on subcontractors

Handling data security incidents:

- Incident response plan
- Notification
- Access

The above refers to data security generally. Refer to the Defence Signals Directorate's (DSDs) *Cloud Computing Security Considerations* for guidance on issues to consider and development of a risk assessment.

- **Business continuity and disaster recovery**

Cloud computing arrangements can raise some very important business continuity and disaster recovery issues as the Agency may have a reduced understanding of how and where its data is stored and its reliance on an uninterrupted service (whether that be a software application or communication network).

It is important that contracts for cloud services address these risks. Some protections that can be included in these contracts include:

  - Ensuring the supplier develops and maintains a detailed and robust business continuity and disaster recovery plan
  - Ensuring the supplier has a geographically separate disaster recovery site with quick ‘failover’ to that site
  - Ensuring the supplier has uninterruptable power supply and back-up generators that allow for uninterrupted service
  - Not allowing the supplier to rely on force majeure provisions unless all business continuity and disaster recovery obligations have been complied with

- **Ownership and access to data**

  It is important for Agency’s to review the service provider’s contract or terms of service carefully. There should be clear provision for customer ownership of the data, and ability to access or transfer it within reasonable timeframes. If it is not clear and appropriate terms cannot be negotiated, then consider whether the data is appropriate for cloud storage.

  Depending on the nature of the data and how it is processed, it may also be necessary to provide for the customer’s ownership of the results of any processing of the data, and limiting the service provider's use solely to that which is necessary for it to fulfil its obligations under the contract.

  The customer should also plan in advance for the end of the contract if circumstances change (if better solutions become available, or the service provider is acquired or goes out of business). The right to retrieve data might not only be business-critical, but also affects legal compliance requirements such as corporate record keeping and litigation (or other regulatory) discovery actions.

  The contract should provide for the customer’s rights to access data and should stipulate:

  - The period of time after termination in which the customer can migrate the data
  - The process for retrieval (if the amount of data is very large, for example)
  - The transition-out assistance from the service provider (even if at additional cost)
  - The format for provision of the data (in particular, not in a proprietary format)

- The requirements for deletion of the data, and sanitisation of the service provider's media
- Any rights of customer audit.

Finally, Agencies may also wish to provide for visibility and oversight of the service provider's:

- Ethics and corporate governance policies
- Disaster recovery and business continuity plans
- Adequacy of insurances.

- **IT Governance**

  The Cloud user should have an appropriate IT governance model to ensure its computing environment complies with all relevant organisational information technology policies. John Sheridan, AGCTO, refers to the possible 'explosion of IT' with the risk that a 'business discovers it has five or six financial management systems [or]…discovers that it doesn't know where its data is [or]…discovers that important corporate data is distributed in the 2013 equivalent of a million Access databases across the organisation'[12].

QUESTIONS?

[12] http://agimo.gov.au/2013/03/18/tomorrow-ready-cio/