Australian Government

AusTender Cloud Migration Business Case and Implementation Strategy

ausTENDER

Document Versioning

Version No.	Date	Description	Authors/contributors
V0.1	19-Feb-2014	Initial draft	s22 [redacted]
V0.2	17-Mar-2014	Initial edits	
V0.3	18-Mar-2014	First draft for client	
V0.4	02-Apr-2014	Reflect Finance feedback	
V0.5	04-Apr-2014	Finance edits	
V0.6	06-Jun-2014	Final format edits	
V0.7	10-June-2014	Adjusted for feedback & corrections.	

Document Details

Document Title	AusTender Cloud Migration Business Case and Implementation Strategy
Document Security classification	Unclassified
Dissemination limiting marking	None
Date of security classification review	Not applicable
Authority	Department of Finance
Author/s	s22 [redacted]
Document status	Draft

Document Purpose

This document seeks to record the considerations relevant to the case for migrating the Australian Government's AusTender application from a traditional dedicated infrastructure model to a Cloud-based model.

The document is intended to reflect the results of comprehensive analysis, thus allowing relevant stakeholders to make informed decisions about such a migration, taking into account both business and technical implications, including in relation to:

- Cost management
- Environment efficiency
- Legal and policy requirements
- Stakeholder interests
- Service performance and continuity
- Data management and security
- Supply management
- System architecture
- System development lifecycle
- Data management
- Integration and interface requirements

This document contains an analysis of the above factors, provides solution options and recommends a preferred approach to moving AusTender to the Cloud.

Table of Contents

1. Executive Summary

AusTender (www.tenders.gov.au) is the Australian Government's central platform for procurement and contracting information. AusTender, which is managed by the Commonwealth Department of Finance (Finance), has been in operation since 2003. Initially, AusTender provided web-based tender document distribution and collection functions – effectively delivering an online service for government agency buyers and would-be suppliers to exchange documents (calls for tender and tender responses) during tender processes.

Since then AusTender's role has expanded and firmly established it as a key source of Government procurement information and a public funds commitment transparency tool for the Australian Government. Today AusTender delivers eight major centralised functions to Australian Government agencies and their market.

AusTender employs dedicated hardware infrastructure to meet computing and storage demands – those demands include ensuring that time-constrained processes (such as tender submission by suppliers) are not interrupted or delayed. The AusTender dedicated hardware is replaced on roughly a four year cycle. The last hardware replacement exercise cost $1.763m in capital expenses.

The expanded role for AusTender, and the associated demands upon the dedicated infrastructure model have highlighted a number of issues. These issues are centred on: a) the need for planned disruptions to services, b) supply difficulties, c) resourcing challenges and d) increasing costs.

These issues associated with the dedicated hardware model coupled with the Australian Government's strategic and policy position to advance the adoption of Cloud services have provided impetus to develop a clearer understanding of the benefits available via this business case document.

The concept of migrating AusTender to a Cloud based infrastructure hosting and related service model is expected to lead to a number of business benefits. The anticipated benefits are:

- Increased service availability and performance
- Increased agility in responding to demands on infrastructure
- Reduced infrastructure-related management and operational overheads
- Reduced costs
- Enhanced infrastructure support services, and
- Alignment with Government policy/strategy.

A number of design criteria have been established to provide a basis for option consideration in regards to migrating the AusTender system from a dedicated infrastructure model to a Cloud-based infrastructure hosting model. The criteria are:

- Preserve or increase application security
- Preserve or increase data security
- All AusTender data must be located on-shore in Australia
- Business continuity protections must be preserved or improved
- Increase agility in dealing with demand for compute/storage fluctuations
- Decrease ongoing AusTender infrastructure costs, and
- Eliminate the need for AusTender hardware acquisition.

A sub-set of the considerations applied to options are summarised in the table below:

	Option 0 Base Case	Option 1 Approach To Market	Option 2 Pilot s22 [redacted] (Recommended)
Option description and key considerations	This option is centred on the continuation of current arrangements, with the foreseeable activities factored in. It serves as a base case for measuring the other options considered.	This option involves undertaking an approach to the market seeking responses in a competitive process. This option has the strength of providing a clear line of sight into the offerings available in the market currently. The weakness of this approach is that it will take additional time and funds to complete.	This option involves establishing the AusTender services in the s22 [redacted] facilities based in Sydney to validate the expected benefits of a Cloud based infrastructure model and to progressively release to Australian Government agencies and decision-makers findings from the Pilot.
Total costs (over 5 years)	$ 7,033,242	$ 2,034,914	$1,123,412
Total savings from Base (over 5 years)	N/A	$ 4,998,328	$ 5,909,830
Return On Investment	N/A	645%	1,493%
Net Present Value (7% discount rate)	N/A	$ 2,226,392	$ 3,818,994

The result of the options analysis undertaken has produced a recommendation that the s22 [redacted] Pilot for AusTender' for a period of 1 year (with an additional 12 months available, if required) to be conducted on the basis that:

a) The option provides the best means of addressing the business issues that were identified with the current model.

b) The economic analysis suggests that this option offers superior value for money.

c) The ease of implementation lends itself to addressing the time constraints related to the existing arrangements, and also offers a degree of confidence that is not available with other suppliers yet.

d) It provides Finance, as a central agency, with an excellent opportunity to provide the sector with experience and insights that will build capability and understanding around Cloud adoption.

The recommendation to conduct a Pilot with s22 [redacted] leaves scope for the Department of Finance to approach the market at the conclusion of the Pilot. This is a recommended course of action as it will ensure that the

services are contested in a local Australian market that currently has scope for additional maturity; maturity that is expected to be realised during the period of the Pilot.

The platform and data security concerns that have been associated with Cloud will be addressed in the recommended option. Throughout the design, implementation and ongoing operation of the s22 Pilot an Australian Signals Directorate (ASD)-accredited information security assessor will be engaged to make an independent assessment of the security controls being employed by the AusTender and s22 teams focussing on the adequacy of their coverage and utilisation in accordance with the Australian Government's Protective Security Policy Framework and Information Security Manual.

An examination of capabilities required to successfully implement the recommended option has been undertaken. In focussing on the organisational capabilities of the AusTender team Project Management, Contract Management and Service Management were considered core to the success and it was found that the team has the required levels of maturity in each of these areas to fulfil the demands of the recommended option.

The required technical capabilities to address the needs of the recommended option have been established with the primary AusTender technology partner s22 has worked on the AusTender system since 2005 and has experience with the architecture and ongoing management of the underlying infrastructure for AusTender. s22 also experienced in the utilisation of Cloud based infrastructure platforms. This experience extends s22 infrastructure arrangements for clients across a range of industries including media, entertainment, travel, hospitality and finance.

Consideration has been given to the activities that would be required to implement the recommended option, and a number of project management aspects have been considered. These include:

- Governance Arrangements
- Scope Management
- Schedule Management
- Cost Management
- Quality Management
- HR Management
- Communications Management
- Risk Management
- Procurement Management
- Benefits Realisation, and
- Stakeholder Management.

A preliminary management plan for each of these aspects has been prepared and included in this document. Upon formal approval to initiate the project these should be reviewed thoroughly by the project team.

The project to implement the recommended option is expected to require 3 months of lapsed time. The deadline for the completion of the project aligns with the conclusion of the current AusTender dedicated hardware, which will terminate on 27 September 2014. This hard constraint is considered the primary risk to the project at this stage.

2. Current Situation

2.1 Background

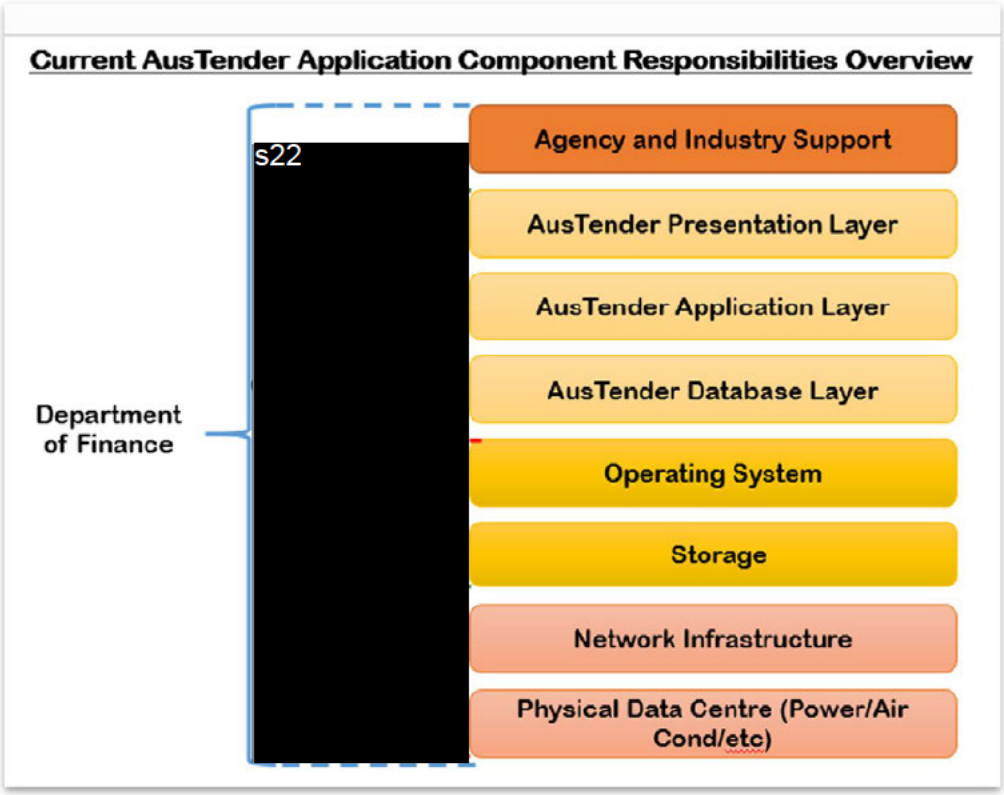
AusTender www.tenders.gov.au is the Australian Government's central platform for procurement and contracting information. AusTender has been in operation since 2003. Initially, AusTender provided web-based tender document distribution and collection functions, effectively serving as an online platform for government agency buyers and would-be suppliers to exchange documents (calls for tender and tender responses) during tender processes.

Since then AusTender's role has expanded and firmly established it as a key source of Government procurement information and a public funds commitment transparency tool for the Australian Government. Today AusTender delivers eight major centralised functions to Australian Government agencies and their market:

1. Planned procurement publication, notification and watch-listing;
2. Publication of publicly available government business opportunities;
3. Automatic notification of those opportunities to suppliers in accordance with self-defined business profiles;
4. Management of restricted tendering processes;
5. Tender documentation and addenda distribution;
6. Secure electronic lodgement of tender responses;
7. Reporting of procurement contracts awarded valued at $10,000 and above; and
8. Associated reports library and searching.

This expansion of AusTender functionality over that period of time has necessitated ongoing expansion in the system's underlying hardware and related infrastructure to ensure suitable service performance levels. The most recent AusTender hardware refresh was undertaken in 2012/13 and required $1.763m in capital costs. The AusTender hardware has been refreshed on a cycle of approximately every four years since its inception.

The roles and responsibilities for the various components and services needed to deliver AusTender are shown below:



According to the US Government National Institute of Standards and Technology (NIST) 'Cloud computing' is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Under this definition Cloud model is composed of five essential characteristics, discussed below:

On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.

2.2 Current Technical Environment

AusTender's current Production environment and Disaster Recovery infrastructure consists of the following components:

Servers in 2 data centres hosting:

- 2 x Load balancers
- 2 x Firewalls
- 8 x Switches
- 2 x SAN disks
- 4 x Web Servers
- 2 x Database Servers
- 2 x Management Servers
- 2 x Tape Drives

The software management approach employed for AusTender also utilises Pre-production, Test, and Development environments.

s22 [redacted] services are provided as part of the hosting service arrangements they provide. The s22 [redacted] services include:

- Web Proxy access – Used to provide secure proxy internet access to the servers for testing and monitoring purposes.
- Network Time Protocol (NTP), Domain Name Service (DNS) – Provide basic network management services from a reliable redundant source.
- Health and Availability Management – Provides monitoring of the servers and services within the environment using NAGIOS and Cacti.
- Protected internet access for the web service using redundant ISP feeds as well as a variety of IPS/IDS protection.

The existing managed infrastructure hosting services agreement with s22 [redacted] for AusTender is scheduled to terminate on the 27th September 2014. There are no further options for extension.

2.3 Business Problem

The ongoing management of AusTender infrastructure has become increasingly complex and costly as the functional offerings of the AusTender services have increased in breadth and depth.

The increased complexity in managing the AusTender infrastructure environment manifests in the following ways:

a) A combination of the number of components and the time and effort to manage each of them necessitates more frequent planned service outages.

b) Hardware manufacturers/suppliers are increasingly less able to satisfactorily meet demands with regards to parts (for example, RAM or local storage drives), expertise and service needed to support the AusTender performance and availability.

c) The existing service model employed for AusTender includes responsibility for two external technology partners with overlapping responsibilities, and the area of overlap presents risks in relation to cost effectiveness, performance and accountability.

d) The time and effort demands on the AusTender team over extended periods of time that are needed to implement new or replacement components into the environment detract from the team's capacity to focus on delivery of core services to Government and Industry stakeholders, specifically a) supporting the efficient and effective engagement of industry and government in procurement processes, and b) publishing timely and accurate information relating to those processes and other procurement related material.

The ongoing and increasing costs associated with managing the current environment is largely due the fact that AusTender is subject to peaks of activity, often with associated sensitive time-constrained business processes that require the environment to possess a large amount of otherwise un-utilised capacity so that it can meet those peak demands. This 'designed-in' over-specification comes with a cost impost that may be able to be addressed by alternate infrastructure service models that offer elasticity of resource allocation.

The following factors have influenced the Department of Finance's decision to consider alternatives to maintaining the current environment:

a) Reduced availability of funding as Government operating budgets are constrained by the overall Australian Government budget position, and

b) The legislative and reputational (and ethical) obligation on Finance to ensure that expenditure of public funds is done in a manner that ensures due economy and that the maximum value for money is extracted. If the cost savings that are apparently associated with Cloud based services are available (and this business case seeks to validate this) they cannot be ignored in the ongoing delivery of AusTender.

Stakeholder Impact

The business issues listed above point to a number of implications for stakeholders.

The implications for Department of Finance/AusTender management manifest as resource challenges (both human and financial) arising from the current hosting arrangements. The human resource dimension relates to challenges arising around the optimal allocation of staff, which have a primary function of ensuring

ongoing service to Agencies and Industry can be redirected to assist with planning and implementation of infrastructure related activities. The financial resource dimension here relates to challenges arising around funds allocation prioritisation between the AusTender program and other programs within the Department of Finance responsibilities.

The public end-user community stakeholders, in particular, participants in tender processes and those seeking information available on AusTender, can experience implications relating to the availability of the service when the need for planned service outages occur to facilitate AusTender infrastructure adjustments. These outages are scheduled to occur outside of normal ACT business hours however the AusTender service does attract visitor traffic at all times of the day so any outage is likely to impact a proportion of the end-user community.

2.4 Current Risks

A number of business and technical risks have been identified with continuation of the dedicated hardware and infrastructure model employed for AusTender.

The AusTender service functional 'footprint' expansion and the related issues described above can be expected to continue on a similar trajectory to that of the past. A concrete example of an anticipated extension of the AusTender system can be found in a new initiative known as 'Dynamic Sourcing for Procurement' (or 'DS4P').

DS4P will allow agency staff to review profile information about suppliers on more than 1,100 existing procurement panels, and where they're authorised, the agency staff will invite a number of the empanelled suppliers to participate in competitive processes – typically Requests for Quote/Proposal/Information/etc. (known generically as RF*x,* where x represents a range of request types).

This new functionality will allow Government agency purchasing personnel to access goods and services from pre-qualified suppliers without having to conduct full scale tender processes, allowing them and industry to avoid the associated costs of tender processes. However, through the online quoting process competitive tension will be able to be maintained to ensure value for money being achieved.

The DS4P functionality is expected to trigger increased use of the AusTender system, mostly because:

a) It will support agency buyers that participate in purchasing activity (conducting RF*x* processes), as distinct from procurement activity (typically conducting traditional open tender processes), and

b) It will attract a greater number of visitors from the supplier community participating in RFx processes.

The increase in the number of RF*x* will largely depend on the uptake of DS4P by Australian Government agencies. There is evidence in the Australian Government of growth in procurement arrangements that concentrate on maintaining competitive tension among a particular supplier group selected from within the broad pool of pre-qualified suppliers. This direction is supported at a policy level by the Government's policy ambitions to ensure effective procurement policy that reduces compliance and participation costs for businesses seeking to provide goods and services to the Australian Government.

2.5 Current Costs

The tables below show the current operating and capital expenses for AusTender.

AusTender Infrastructure Related Existing Capital and Recurrent Costs

Schedule of Capital Costs

Cost source	Total cost of most recent hardware refresh in 000's	Annualised hardware refresh costs in 000's
Hardware	$757.6	$189.4
HW Implementation Costs	$1,005.7	$251.4
Total capital expenditure	*$1,763.3*	*$440.8*

Schedule of Operating Costs

Cost source	Monthly Costs excl. GST in 000's	Annual Costs excl. GST in 000's
Existing Hosting Managed Service Provider s22	$23.0	$276.0
Existing Application Service Provider Infrastructure-specific Effort s22	$3.9	$46.5
Other	$14.0	$167.8
Total recurrent expenditure	$40.9	$490.3

Notes

* Department of Finance internal costs such as staff and facilities are excluded from the above calculation as they are not expected to change as a result of the migration from dedicated to Cloud-based infrastructure.

* The existing hosting service provider costs include: hosting, gateway, operating system management.

* The application service provider's infrastructure-specific costs are represented here, and distinguished from software related activities.

* The 'Other' costs are derived from AusTender's costs derived from other sources, such as software licences, security certificates and software/OS vendor support arrangements.

3. Proposed Response

3.1 Strategic Alignment

The Australian Government policy position in relation to Cloud adoption is the 'Australian Government Cloud Computing Policy — Maximising the Value of Cloud' released in May 2013'

The Australian Government agencies will:

- *Consider Cloud services for new ICT procurements. Agencies will choose Cloud services where the Cloud service represents the best value for money and adequate management of risk compared to other available options;*
- *Commence procurement of public Cloud services for their testing and development needs, as appropriate where the service represents the best value for money and is fit for purpose;*
- *Transition public facing websites to public Cloud hosting at natural ICT refreshment points, where those Cloud services demonstrate best value for money and is fit for purpose; and*
- *Establish information sharing initiatives to facilitate continual improvement based on a repository of case studies, better practices risk approaches and practical lessons to enable agencies to learn from each other*

The policy provides a set of practical considerations for agencies to consider in their decision making in relation to adopting the public Cloud, as follows:

In becoming a leader in the use of Cloud services, Australian Government agencies will consider the following factors when procuring Cloud services:

a) *Value for money – including that the service is fit for purpose - as defined in the Commonwealth Procurement Rules;*

b) *Adequate security - as defined in the Protective Security Policy Framework;*

c) *Delivering better services - as detailed in the APS ICT Strategy 2012-2015;*

d) *Improving productivity - as detailed in the APS ICT Strategy 2012-2015;*

e) *Achieving greater efficiency - as detailed in the APS ICT Strategy 2012-2015; and*

f) *Developing a more flexible workforce.*

Each of these practical considerations is addressed further in this document.

A number of other Australian Government policy initiatives are relevant to the AusTender Cloud Migration initiative. They are listed below:

National Digital Economy Strategy
The National Digital Economy Strategy aim is that, by 2020, Australia will be among the world's leading digital economies. The strategy identifies the role Cloud computing can play in reducing the cost of ICT to government and the improvement in service delivery to business and individuals.

National Cloud Computing Strategy
The *National Cloud Computing Strategy* complements the *National Digital Economy Strategy* and examines the broad role of Cloud technologies, the various opportunities and potential for the nation (private, public and not for profit sectors) and includes a section on the 'Government's use of Cloud Computing' in the context of the wider Australian economy.

The strategy identifies Cloud computing as a key enabler of the digital economy and addresses the barriers to adoption of Cloud computing by setting out a range of actions to accelerate the adoption of Cloud services across the sectors.

Australian Public Service ICT Strategy 2012-2015
The *Australian Public Service ICT Strategy 2012-2015* outlines how Australian Government agencies will continue to use ICT to drive better service delivery, improve government operations, drive productivity, and to engage with people, the community and business. It supports better, more accessible government services for people when, where and how it suits them, so they can be more productive.

The strategy recognises the benefits Cloud computing provides to increased capability and improvement of efficiency through lower customisation and integration costs to government operations.

3.2 Technical Environment

The AusTender technical environment is considered well suited to Virtual Private Cloud-based hosting.

This view has been established via a technology focussed Proof of Concept initiative that was completed in early 2014. That initiative sits among a broader program of work focussed on the duplication, rebranding and adjustment of the AusTender application to become a separate application serving as the Australian Government's grants management and information service.

The relationship between AusTender and a Grants Reporting system is premised on the conceptually similar business processes within procurement and grants management. It is expected that the policy and regulatory findings during this 'AusTender Cloud Migration Business Case' will provide a number of substantial inputs into the grants.gov.au program – and thereby eliminate or reduce the need for duplication of activities under that program.

A copy of the Proof of Concept Evaluation Report is available upon request from the AusTender team. In summary the proof-of-concept's (PoC) evaluation report found the following:

The PoC has shown that it is technically feasible to use Virtual Private Cloud-based hosting for the grants.gov.au or tenders.gov.au sites. System architecture was developed s22 *with similar levels of redundancy & security to that of the current tenders.gov.au hosting infrastructure.*

The performance of the PoC site also showed that there may be benefits to the end-user by running the sites on more powerful infrastructure. Load tests showed that the site's pages appear to load much faster, and experiments showed that the current limits on report download datasets may be able to be lifted so that users can produce bigger reports from the site without any impact.

s47E

Cost savings may be possible due to the need for a reduced number of servers and the ability to dynamically adjust the level of compute power required to service the site. A full business case will be required to determine the total economic benefits of virtual vs physical hardware.

3.3 Anticipated Business Benefits

The concept of migrating AusTender to a Virtual Private Cloud based infrastructure hosting and related service model is expected to lead to a number of business benefits. These benefits are discussed below.

- **Increase service availability and performance** – specifically establishing a robust technology architecture that supports high availability delivering business continuity, and service performance that supports load with minimal performance degradation regardless of peak demand spikes

- **Increase agility in responding to demands on infrastructure** – overcome time delays associated with acquiring and implementing dedicated hardware, and avoid the limited manufacturer inventory constraint challenges associated with upkeep of dedicated servers.

- **Reduce infrastructure-related management and operational overheads** – specifically the opportunity to shift from the need for substantial capital expenditure projects associated with regular hardware refreshes to an operating expenditure model that does not divert resources away from frontline service delivery

- **Reduce costs** – this objective refers to costs associated with hosting facilities, hosting support services, as well as the costs driven by hardware refresh events involving hardware acquisition and implementation.

- **Enhance infrastructure support services** – improved visibility and accountability in the governance structures around infrastructure for AusTender to enable effective 3rd party supplier management

- **Align with Government imperatives** – support policy objectives relating to adoption of Cloud-based technologies.

4. Solution Options

4.1 Design Criteria

The following list of mandatory and optional solution criteria provides guidance on the option assessments.

Mandatory Criteria:

- Preserve or increase application security
- Preserve or increase data security
- All AusTender data must be located on-shore in Australia
- Business continuity protections must be preserved or improved
- Increase agility in dealing with demand for compute/storage fluctuations
- Decrease ongoing AusTender infrastructure costs, and
- Eliminate the need for AusTender hardware acquisition.

4.2 Identified Options

The following section of the document explores a broad set of considerations for three different options available to the Department of Finance in relation to AusTender infrastructure services.

Option 0: Base Case

Description: This option is premised on the AusTender infrastructure remaining under the current hosting arrangements and model.

Stakeholder Impacts: As per the impacts discussed above in section 2.3, the primary impacts for agency and public users under this option centre on planned service disruptions to manage the dedicated infrastructure. The Department of Finance is impacted under the 'Do Nothing' option in that the management overhead associated with dedicated hardware provides a resource allocation challenge whereby key staff are redirected from core service delivery efforts to instead manage hardware refresh cycles. Additionally funding dedicated infrastructure runs counter to Department of Finance and broader Australian Government policy objectives.

Costs: As per existing model, with considerable OPEX and cyclical 'spikes' in CAPEX required for hardware refresh and hardware expansion. A model of the likely costs for this option is shown below.

Option 0: Base Case

Schedule of Capital Costs

Cost Items	Year 0 in '000s	Year 1 in '000s	Year 2 in '000s	Year 3 in '000s	Year 4 in '000s	TOTAL OVER 5YRS in '000s
Hardware	$757.6	$170.5	$0.0	$0.0	$833.3	$1,761.4
Implementation Services	$1,005.7	$226.3	$0.0	$0.0	$1,106.3	$2,338.3
Total Capital Costs (CAPEX)	$1,763.3	$396.7	$0.0	$0.0	$1,939.6	$4,099.7

Schedule of Recurrent Costs

Cost Items	Year 0 in '000s	Year 1 in '000s	Year 2 in '000s	Year 3 in '000s	Year 4 in '000s	TOTAL OVER 5YRS in '000s
System Hosting Services	$276.0	$331.2	$339.5	$348.0	$356.7	$1,651.3
Application Hosting Services	$46.5	$55.8	$57.2	$58.6	$60.1	$278.3
3rd Party Software Licences	$167.8	$201.4	$206.4	$211.6	$216.8	$1,004.0
Total Recurrent Costs (OPEX)	$490.3	$588.4	$603.1	$618.2	$633.6	$2,933.6
Total OPEX and CAPEX	$2,253.6	$985.1	$603.1	$618.2	$2,573.3	$7,033.2

Assumptions and Notes

* All figures are in Australian dollars without GST applied.

* Assumes a Year 1 minor (20%) HW expansion to cater for introduction of new functionality (specifically DS4P) and the related load and utilisation increases associated with that. The same increase in system hosting/services costs and licence costs is also added from Year 1.

* Recurrent costs are assumed to rise @2.5% annually. Capital costs are assumed to have increased by a straight 10% over the 4 years between hardware refresh initiatives. This is considered quite conservative because the inflation is not compounded over these 4 years and there are expectations that dedicated HW on this scale will become more costly as the market dynamics change with increasing Cloud utilisation and reduced use of dedicated hardware of the sort employed by AusTender.

Savings: Not applicable to this base case because it is premised on no change to the existing arrangements.

Benefit: The key benefit to this option is that with no change in existing arrangements no Cloud migration exercise would be necessary.

Risk: Ongoing risks to service availability, service performance and hardware management challenges have been identified in the discussion above.

Timeframe: The existing hosting managed services arrangement with s22 terminates on 27 September 2014. The agreement with s22 is based on a term of 2 years plus an option for an additional 12 months. The Department of Finance exercised the final option in September 2013, so a new arrangement would be necessary to extend beyond September 2014.

Option 1: Approach to Market

Description: This option centres on the means by which the Department of Finance might procure alternate Cloud services for AusTender through an open approach to the market to seeking suitably skilled and experienced service providers to provide the ongoing infrastructure management of AusTender. Under this option, the Approach to Market (ATM) would seek to address the risks identified above with the existing arrangements, and would therefore focus on seeking responses specifically from 'Cloud' services providers that could address the design criteria outlined above.

Key among the considerations relevant to the acquisition of these services are the existing procurement instruments available to the Department of Finance and adherence to the Australian Government's Commonwealth Procurement Rules.

Stakeholder Impacts: This approach would generate interest from a wide range of would-be suppliers across the Australian and international Cloud service provision sector, and would likely generate local media attention as it could be taken to signify a step towards Cloud hosting adoption for a whole-of-government web application with a significant profile across industry and the Australian Government sector.

Costs: An ATM is considered a costly means of acquisition for both the agency involved and the supply community that participates in the tender process; however this cost must be considered against the objective to achieve maximum value for money in the expenditure of public funds.

Conducting an open approach the market seeking a suitably capable and experienced Cloud Service Provider is conservatively estimated, based on past experience and industry benchmarks, to cost approximately $300k and estimated to take 6 months in duration from end-to-end.

Accordingly this cost and the necessary extension of the existing arrangements for a suitable duration to allow for a procurement process to be conducted has been reflected in investment costing model set out in the table below.

Option 1: Approach to Market Cost Model

Schedule of Capital Costs

Cost Items	Year 0 in '000s	Year 1 in '000s	Year 2 in '000s	Year 3 in '000s	Year 4 in '000s	TOTAL OVER 5YRS in '000s
Hardware	-	-	-	-	-	-
Implementation Services	-	$371.0	-	-	-	$371.0
Acquisition Process Costs	$300.0		-	-		$300.0
Total Capital Costs (CAPEX)	$300.0	$371.0	-	-	-	$671.0

ausTENDER

Schedule of Recurrent Costs

Cost Items	Year 0 in '000s	Year 1 in '000s	Year 2 in '000s	Year 3 in '000s	Year 4 in '000s	TOTAL OVER 5YRS in'000s
System Hosting Services	$276.0	$195.2	$60.4	$60.4	$60.4	$592.0
Application Hosting Services	$46.5	$49.3	$43.8	$44.9	$46.0	$184.5
3rd Party Software Licences	$167.8	$117.1	$63.8	$65.3	$67.0	$414.0
Total Recurrent Costs (OPEX)	$490.3	$361.5	$168.0	$170.7	$173.4	$1,190.5
Total OPEX and CAPEX	$790.3	$732.5	$168.0	$170.7	$173.4	$2,034.9

Assumptions and Notes

* All figures are in Australian dollars without GST applied and where they have been converted from USD an exchange rate of AUD$1.15 = USD$1.00 is assumed.

* Assumes that during Year 0 current hosting and related costs continue whilst the Approach to Market process takes place, and this process is costed at $300k based on experience with similar procurement processes. In Year 1 it is assumed that transition to the Cloud will take 6 months and during that period the current recurrent costs remain relevant, and for the remaining 6 months of that year it is assumed that Finance will pay Cloud-based hosting costs. Year 1 also assumes an implementation cost that incorporates technical, regulatory and economic feasibility effort as well as the effort of migrating to the Cloud infrastructure.

* Recurrent costs are assumed to rise @2.5% annually, except for the Cloud Hosting costs which are assumed to remain stable.

Savings: Considerable cost savings appear to be available in the cost modelling conducted for this option. Over a 5 year period the current costs are expected to total $7.03m, whereas the modelling for this option suggest a total cost over the same period of $2.03m, indicating total potential savings of $4.998m over 5 years.

Benefits: The primary benefit of an open approach to the market is that it would allow the AusTender team to establish from among a broad range of Cloud service suppliers a clear indication of capability and costs for the required services.

Summary Cost Benefit Analysis: An examination of these options has been undertaken with both Return on Investment and Net Present Value calculations having been made, and are presented below.

Return on Investment	ROI over 5 years
Current costs over period	$7,033,242
Proposed costs over period	$2,034,914
Gross savings from investment over period	$4,998,328
Cost of Investment	$671,000
% Return on Investment	645%

Net Present Value (NPV)

The following tables display the Net Present Value calculations associated with the migration of AusTender from the current arrangements to the ATM option.

NPV at with discount rates of 5%, 7% and 10%			
Initial investment (includes PoC, Bus Case ATM and Implementation effort) = $671,000			
	Do nothing CAPEX+OPEX	ATM CAPEX+OPEX	Yearly Savings (Do nothing CAPEX + OPEX) less (ATM Option CAPEX +OPEX)
Year 1	$2,253,619	$790,314	$1,463,305
Year 2	$985,120	$732,533	$252,588
Year 3	$603,086	$167,977	$435,109
Year 4	$618,163	$170,667	$447,497
Year 5	$2,573,253	$173,423	$2,399,830
NPV @ 5%	$2,408,556		
NPV @ 7%	**$2,226,392**		
NPV@ 10%	$1,987,348		

NPV is a financial appraisal method that can be universally applied to make an assessment about the economic feasibility of a proposed investment. The calculation of NPV applies the principles of discounted cash flow where future cash flows are multiplied by a discount rate to obtain present values. As a general rule where an NPV value is positive that is regarded as a sign that the investment is worthwhile, whereas a

negative NPV would indicate that the investment should not proceed without the identification of substantial unquantifiable benefits.

These results for ROI and NPV suggest a strong case for this option from a financial perspective. Typically it would be necessary to undertake sensitivity analysis to these calculations to ensure that the option remains viable if the expected costs were to be higher or the expected benefits were to be lower than the model predicts.

In this case it has been established that the costs would need to be wrong by a factor of about 2.9 times to bring the NPV down to zero. The cost components that are likely to vary in a case like this are implementation costs, currency fluctuations and service fees. Since a 290% increase in costs is unlikely no further sensitivity analysis is provided here, but that analysis is available upon request.

Risks: An existing procurement arrangement known as the 'Data Centre as a Service Multi Use List' includes a number of suppliers able to provide Cloud and Cloud-like services to Australian Government entities wishing to procure services valued at less than $80k and for a term not lasting for longer than 12 months. The Data Centre as a Service (DCaaS) Multi-Use List (MUL) is managed on behalf of the Commonwealth of Australia (Commonwealth) by Finance.

The transition of the AusTender hosting arrangements to one of the 80 suppliers on the DCaaS MUL are not considered appropriate at this stage. This is primarily because the cost and term of the engagement are expected to exceed the limitations under which the MUL operates. Additionally, it is worth noting that the DCaaS MUL was introduced as a trial for two years, and is due to expire on 30 October 2014. The DCaaS is not expected to continue in its current form, and it is expected to be overhauled by the end of 2014 although no formal position has been taken on potential adjustments in such a subsequent arrangement, or whether a comparable arrangement will be created. With the existing AusTender hosting arrangements due to terminate in late September 2014, the use the DCaaS is considered to significantly heighten the AusTender Cloud migration objective risk at this point in time. So with no other appropriate existing procurement arrangement in place the Department of Finance has the option to conduct an open approach to the market.

The number of service providers in Australia that identify themselves as 'Cloud' service providers is significant. However, 'Cloud' is a broad term that is used extensively by market participants without necessarily having a shared definition. An open procurement process would need to be designed to discern among the potential market participants a clear pathway for Finance to adopt the most suitable Cloud service 'variant', and necessary time and resources required to conduct such a process are considered a risk to objectives.

An additional risk consideration if an open procurement process were to be undertaken is that a wide audience would need to be made familiar with the AusTender application security controls. Whilst the nature of commercially sensitive content passing through the AusTender system is not classified under the definitions provided in the 'Information Security Management Guidelines', some of the information contained in the system is considered 'For Official Use Only' because unauthorised release could cause limited damage to commercial entities, and potentially engender distrust of government information management practices in procurement processes. On that basis it is not considered appropriate to publish details of the system architecture in the public domain via an open tender. Whilst concerns such as these are typically addressed via multi-stage processes with a progressive divulgence of sensitive information as the field of suitable contenders narrows, in this case the time-frame considerations, discussed below, do not provide sufficient scope for adoption of that approach.

Timeframe: As mentioned, the Australian Government has established a Cloud strategy that encourages all agencies to transition public facing web sites to the public Cloud where natural refreshment points occur (among other considerations). While this can be interpreted as the point in time that the next hardware refresh would have normally occurred, so that the capital assets that the hardware represents has been fully depreciated. Unless the hosting services agreement in place for dedicated infrastructure arrangements has a term that aligns with the asset's depreciation schedule, a natural point for applications such as AusTender to consider the transition to the Cloud is at the end of the term of the agreement with the current hosting services provider. In AusTender's case this is late September 2014.

Also described above is that the end-to-end process is expected to take 6 months; that period of time would require a number of internally and externally sourced inputs for various activities including detailed requirements documentation along within a suitable Request for Tenders documentation framework, as well as the providing industry adequate time to digest and respond to those requirements, and then a suitable period to evaluate those responses against pre-determined evaluation criteria and finally to form an agreement with a suitable provider. Once the agreement is established a period of time would be necessary to effect the process of transition itself.

With the current AusTender infrastructure hosting arrangement in place until late September 2014, the period for the ATM and then the subsequent negotiations followed by implementation mean that detailed project schedule planning and careful project control and monitoring would be necessary to be achieved in the available time.

Option 2: Pilot with s22 then ATM

This option centres on conducting a Pilot or trial with s22 to thoroughly explore the implications and benefits of adopting a Virtual Private Cloud-based infrastructure for AusTender and provide an accurate verification of the benefits anticipated of Cloud adoption.

Description: The Department of Finance has the option of undertaking a trial with s22 establish a substantial case study for the Australian Government in the adoption of Virtual Private Cloud services using the AusTender Cloud infrastructure hosting transition as the study subject.

The technical feasibility work that has been conducted with AusTender in the s22 environment as a proxy for the forthcoming grants.gov.au system makes this option a possibility. s22 consistently ranked as the most mature and capable Virtual Private Cloud services provider by independent ICT researchers, such as s22

The s22 as a strong industry leader, in relation to their measures of a) completeness of vision and b) ability to execute that vision. The leading position that s22 holds on these measures is clearly demonstrated in the diagram below:

s22

In terms of policy considerations, a Pilot with s22 would be required to satisfactorily address the practical aspects set out in the policy (specifically 'Australian Government Cloud Computing Policy — Maximising the Value of Cloud' released in May 2013'). Each of these aspects are discussed below.

Value for money: The factors for consideration under the Commonwealth Procurement Rules pertinent to achieving value for money are listed below with discussion on each related to this option.

Fitness for purpose: The s22 ervices have been established as providing a technically feasible model for hosting AusTender via the grants.gov.au program preliminary analysis, and s22 service model would allow Finance to address each of the mandatory design criteria outlined above.

A potential supplier's experience and performance: The experience and performance of s22 indicated by the independent research outlined above suggests that they are a capable provider.

Flexibility including innovation and adaptability over the life-cycle of the procurement: Virtual Private Cloud platforms generally provide in flexibility because the model of delivery is itself premised on an inherent flexibility – that is, no limitations on the ability to scale up and down in response to changing business needs. In relation to innovation and adaptability, certainly the intent of a Pilot would seek to identify opportunities for innovation in a public Cloud environment as distinct from AusTender's existing dedicated hardware model. Of particular consideration under a trial or Pilot would be the ability of Finance to transition out s22 to other Virtual Private Cloud providers or to other infrastructure hosting models

should that be considered appropriate at any given time s22 does offer that degree of adaptability in that the contractual arrangement is not for a fixed term. From a technical perspective, an effective transition out s22 would require a detailed 'transition out' planning exercise; however, when considering financial aspects (in particular the notion of "vendor lock-in" - where the cost/inconvenience/disruption of terminating arrangements with a specific vendor become prohibitive) it is understood that there are minor technological nor financial inhibitors that would need to be overcome to step away from s22 the end of a Pilot should that be considered necessary; in fact the s22 cost of retrieving the entire AusTender data set at its current volume, would cost approximately $AUD130.

Whole of life costs: The concept of whole-of-life becomes difficult to apply once the costs associated with the capital expenditure on a regular dedicated hardware refresh cycle are transferred to operating expense under a Cloud arrangement. However, for the purposes of comparison this business case has uniformly applied a 5 year period benchmark for cost comparisons. This subject is addressed more fully further on in this document, but in summary the cost modelling over 5 years suggests a cost reduction of $5.9m with s22 compared with the existing arrangements over the same period.

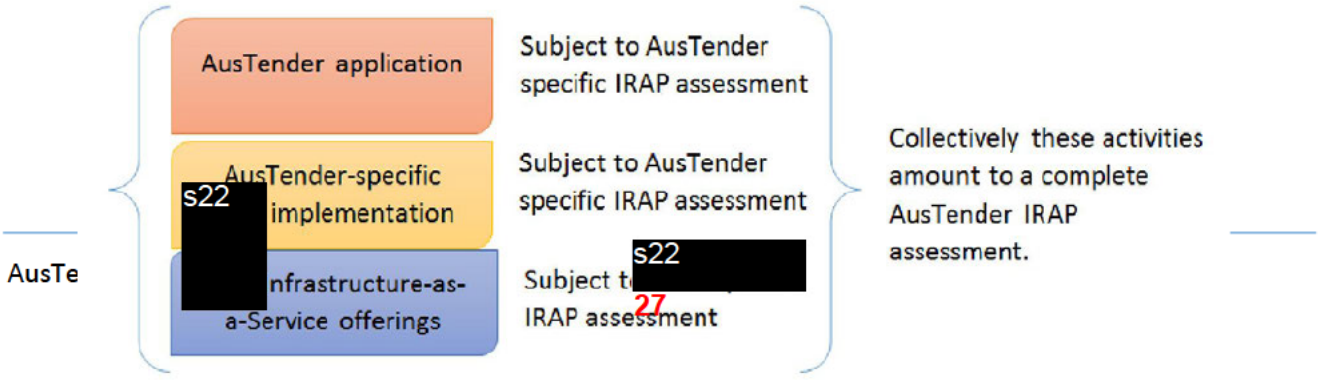
Adequate security *(as defined in the Protective Security Policy Framework or PSPF)*: The PSPF, administered by the Attorney-General's Department, is premised on core mandatory requirements covering governance, personnel security, information security and physical security. The PSPF is complemented by the Australian Signals Directorate's (ASD) standard set of principles and controls that govern the security of government ICT systems – that standard is named the Information Security Manual (ISM).

The Information Security Registered Assessors Program (IRAP) is an ASD initiative to provide high quality information and communications technology (ICT) services to government in support of Australia's security. ASD endorses qualified ICT professionals, against ASD requirements, to provide quality ICT security services aiming drawing on the ISM to best secure Australian Government information and associated ICT systems.

IRAP provides the framework to endorse individuals from across the private and public sectors to provide cyber security assessment services to Australian Government agencies. Endorsed IRAP Assessors will provide an independent assessment of ICT security, suggest mitigations and highlight associated residual risk. It is the aim of IRAP to assist in safeguarding Australian Government information.

At the time of this document being authored s22 was undertaking a comprehensive IRAP assessment, with the intention of having the core s22 platform offerings accredited or recognised by ASD as meeting ASD prescribed levels of security.

Under the AusTender model, the infrastructure that s22 provides is pending the outcome of that IRAP assessment. However, that IRAP assessment scope addresses only the s22 environment generically. Therefore, a further information security assessment that focuses on the specific combination of s22 and AusTender application will be necessary. Effectively, this will require an IRAP assessment of the areas of the overall AusTender platform s22 that are not addressed by the generic s22 IRAP assessment. Based on the grants.gov.au proof-of-concept, a preliminary IRAP assessment has been made of the AusTender application in s22 environment, so the areas of particular focus and the pathway to complete that assessment have been determined. This is represented in the diagram below:



Stakeholder Impacts: As described above, it is expected that this option would allow AusTender staff and the Department of Finance more broadly to better focus activities on policy objectives related to AusTender.

This option would be expected to decrease the number of planned AusTender outages, and this would be a positive impact for the industry stakeholder group that rely on AusTender as a source of information and a means of responding to Australian Government business opportunities.

Costs: A costing model for this s22 a Pilot option has been prepared. Although it is not suggested that the Pilot run for 5 years, the cost model has been created over that timeframe so that it can be compared with the other option on a like-for-like basis.

Option 2: Pilot with s22

Schedule of Capital Costs

Cost Items	Year 0 in '000s	Year 1 in '000s	Year 2 in '000s	Year 3 in '000s	Year 4 in '000s	TOTAL OVER YRS 1 to 5 in $AUD '000s
Hardware	$ -	$ -	$ -	$ -	$ -	$ -
Implementation Service Fees	$ 371.0	$ -	$ -	$ -	$ -	$ 371.0
Total Capital Costs	$ -	$ -	$ -	$ -	$ -	$ 371.0

Schedule of Recurrent Costs

Cost Items	Year 0 in '000s	Year 1 in '000s	Year 2 in '000s	Year 3 in '000s	Year 4 in '000s	TOTAL OVER YRS 1 to 5 in $AUD '000s
System Hosting Services	$114.3	$ 60.4	$ 60.4	$ 60.4	$ 60.4	$ 355.9
Application Hosting Services	$ 42.8	$ 42.5	$ 43.6	$ 44.7	$ 45.8	$ 219.4
3rd Party Software Licences	$ 62.2	$ 27.7	$ 28.4	$ 29.1	$ 29.8	$ 177.1
Total Recurrent Costs	$ 219.3	$ 130.6	$ 132.4	$ 134.2	$ 136.0	$ 752.4
Total CAPEX and OPEX	$ 590.3	$ 130.6	$ 132.4	$ 134.2	$ 136.0	$ 1,123.4

Assumptions and Notes

* All figures are in Australian dollars and where they have been converted from USD an exchange rate of AUD$1.15 = USD$1.00 is assumed.

* 'Year 0' is modelled on 3 months of existing recurrent costs then switches for the following 9 months to reflect s22 hosting costs.

* Ongoing costs are assumed to rise @2.5% over future years for Service and Licences components. s22 Hosting costs have actually decreased many times over the past 6 years (most recently in March 2014 after the preparation of these cost models), so this model assumes neither inflation nor deflation on that cost component. In reality it is expected that currency fluctuation will be the biggest influence s22 costs. Cost variance is discussed further in the NPV section below.

* The Year 1 capital costs represent the estimated costs of planning (including technical feasibility and business case preparation efforts) and then implementing the transition of AusTender to s22 Cloud environment.

Savings: The savings available under this s22 Pilot cost model suggest that total savings across OPEX and CAPEX for the 5 year period would be $5.91million based on the costs of the existing arrangements.

Benefit: Apart from the significant economic benefits identified in the savings section above, there are a number of benefits that are difficult to quantify in this option. The discussion below looks at these benefits through the lens of the Australian Government ICT Strategy 2012-2015, which allows us to focus on better services, heightened efficiency and heightened productivity.

Delivering better services: The strategy identifies service delivery improvement as one of the practical considerations. The utilisation of Virtual Private Cloud infrastructure will address the current situation where planned service outages during periods when users might like to access the service impact service delivery for those involved. On-demand Cloud services would mean that disruption to AusTender services would be greatly reduced. Should a policy or demand-driven event increase the load on AusTender in terms of computing needs or storage needs (or both), AusTender will be well placed to respond almost immediately.

Improving productivity and efficiency: The adoption of s22 Virtual Private Cloud based infrastructure offers Finance the potential for a flexible and cost-efficient hosting solution whilst also freeing resources to focus on the policy and business outcomes on which the provision of the AusTender service is premised; this contrasts markedly with the existing arrangements that requires Finance's AusTender staff to be diverted onto capital expenditure management and hardware asset acquisition/management/disposal activities for extended periods based on the hardware asset management life-cycle, and also the emergent demand-driven or policy adjustment driven activities that 'cut across' that life-cycle.

Summary Cost Benefit Analysis: An examination of s22 Pilot option has been undertaken with both Return on Investment and Net Present Value calculations having been made.

aus TENDER

Return on Investment

Return on Investment	ROI over 5 years
Current costs over period	$7,033,242
Proposed costs over period	$1,123,412
Gross savings from investment over period	$5,909,830
Cost of Investment	$371,000
% Return on Investment	1,493%

Net Present Value (NPV)

The following table displays the Net Present Value calculations associated with the migration of AusTender from the current arrangements to the ATM option.

NPV at with discount rates of 5%, 7% and 10%.			
Initial investment (includes Proof of Concept, preliminary IRAP assessment, Business Case and Implementation effort) = $ 371,000			
	Do nothing CAPEX+OPEX	Proposed CAPEX+OPEX	Yearly Savings (Do nothing CAPEX + OPEX) less s22 CAPEX +OPEX)
Year 1	$ 2,253,619	$ 501,613	$ 1,752,007
Year 2	$ 985,120	$ 130,613	$ 854,508
Year 3	$ 603,086	$ 132,368	$ 470,718
Year 4	$ 618,163	$ 134,167	$ 483,996
Year 5	$ 2,573,253	$ 136,011	$ 2,437,242

NPV @ 5%	$ 4,061,748
NPV @ 7%	$ 3,818,994
NPV@ 10%	$ 3,495,831

NPV is a financial appraisal method that can be universally applied to make an assessment about the economic feasibility of a proposed investment. The calculation of NPV applies the principles of discounted cash flow where future cash flows are multiplied by a discount rate to obtain present values. As a general rule where an NPV value is positive that is regarded as a sign that the investment is worthwhile, whereas a negative NPV would indicate that the investment should not proceed without substantial unquantifiable benefits. As with the ATM approach, the s22 Pilot ROI and NPV figures modelled are very strong and provide a compelling case for decision-makers. The sensitivity analysis to ensure that the figures remain favourable in circumstances where costs are larger than anticipated provide a high degree of confidence that the investment decision will remain sound. The sensitivity modelling that has been done suggests that either s22 option implementation costs could increase 10-fold or the ongoing operational costs of s22 option could increase by 600% and the NPV would remain positive; this suggests that any concerns about future cost variance including currency fluctuations (s22 an international operation charges in USD for all services globally) can be readily discounted.

Risk: The reliance upon the timely and satisfactory conclusion of s22 IRAP assessment is a risk to this option. Should s22 not be able to gain confirmation from an independent assessor that their services are adequately secure, then the validity of the option would be greatly jeopardised.

The initiation of a project to migrate AusTender infrastructure s22 would be dependent upon this aspect being addressed satisfactorily.

Timeframe: The time required to implement AusTender in s22 environment would need to be carefully planned out and scheduled using proper project management principles. However, the experience from the proof-of-concept suggests that the overall timeframe will not exceed 3 months.

4.3 Options Analysis Summary

Requirement	Option 0 Base Case	Option 1 ATM	Option 2 Pilot with s22
Benefits	The existing arrangements would continue so the benefit with this option is that it is a known situation and there would be no effort required to adapt to a new arrangement/model.	An opportunity to be provided with a whole-of-market view of the Cloud Service providers in Australia and their various capabilities.	An opportunity to establish for the Australian Government a substantial case study into the possibilities and considerations of a Virtual Private Cloud migration, which would inform future decision-making, and be an opportunity to verify and validate some of the stated benefits around Cloud arrangements. The fact that this approach has been subjected to a technical feasibility proof-of-concept certainly lowers the risk profile for implementation.
Disadvantages	Cost and inflexibility	Time required to establish a suitable provider and then to validate the capability of the AusTender application to function in that environment.	Other market providers may resent not having had the opportunity to participate in this Pilot, although the intention of the Pilot would be to aid the transition of Government services to Cloud hosting models generally (not exclusively s22 so these market participants would be expected to benefit from this approach in the longer term.
Total costs (over 5 years)	$ 7,033,242	$ 2,034,914	$1,123,412
Total savings	N/A	$ 4,998,328	$ 5,909,830
Return On Investment	N/A	645%	1,493%
Net Present Value (7% discount rate)	N/A	$ 2,226,392	$ 3,818,994

Flexibility of the contract	Fixed contract 2yrs + 1 x 12months option; the option was exercised in 2013 and the additional 12 months option expires on 27th Sept 2014.	Not determined, ATM would establish this based on ATM requirements and/or commercial model of selected supplier.	Flexible – 1 month notice for termination
Estimated implementation timeframe	N/A base case, although ongoing hardware asset management cycle.	6 months	3 months
Preserve or increase application security	Under the existing model application security controls are considered adequate	Potentially depending on provider responses	Yes, increased security based on IRAP assessment outcomes and revised infrastructure model
Preserve or increase data security	Under the existing model data security controls are considered adequate	Potentially depending on provider responses	Yes increased security based on IRAP assessment outcomes and revised infrastructure model
All AusTender data must be located on-shore in Australia	Under the existing model all data is stored on-shore in Australia	Potentially depending on provider responses	Yes all data will be stored in s22 'Australian Region' across two different zones for redundancy
Business continuity protections must be preserved or improved	Existing business continuity model would continue	Potentially depending on provider responses	Yes the use of two zones for redundancy
Increase agility in dealing with demand for compute/storage fluctuations	No - low agility and increasing difficulty in timing sourcing and provisioning of hardware	Potentially depending on provider responses	Yes s22 support model supports elasticity to respond to demand spikes
Decrease ongoing AusTender infrastructure costs	No increased costs expected	Potentially depending on provider responses.	Yes, modelling suggests overall reduction in costs over 5 years of $ 5,909,830
Eliminate the need for AusTender hardware acquisition	Ongoing additional hardware acquisition required	Potentially depending on provider responses	Yes no need for further capital expenses
Implementation risks	Service disruption, and resource challenges	The ATM process itself presents a timing risk with the current hosting arrangements ceasing in Sept 2014.	A dependency on s22 IRAP assessment concluding with satisfactory results.

Conclusion	The costs and the identified business problems effectively render this option non-viable. It is clear from the considerations in this document that Finance should take the opportunity presented by the coming termination of current hosting arrangements to adopt Cloud based infrastructure hosting.	This option has appeal in that the market participants would have an opportunity to furnish Finance with a comprehensive view of the various Cloud service provision capabilities. This option also suggests that significant savings are available compared to the base case - this is evidenced by the very compelling ROI and NPV figures. The timing risk is a real one that will make the ability to achieve a successful migration - without the ongoing costs to the taxpayer being extended - very difficult.	The outstanding NPV and ROI results for this option as well as the additional $911,502 in savings over 5 years that this option presents over ATM Option 1 is very compelling. Also the greater certainty in terms of the implementation path, made available via the earlier proof-of-concept work, for this option make it preferable to Option 1.

4.4 Recommended Option and Rationale

The s22 Pilot option is recommended, however with limitations. The recommended limitations are made with regard for a) the expected advances in maturity of Australia-based Virtual Private Cloud offerings, and b) the expected adjustments to the Australian Government procurement policy framework and procurement arrangements in relation to Cloud services. Therefore it is recommended that the s22 Pilot for AusTender extend for a 1 year period (with an additional 12 months available, if required).

The rationale for the recommendation is based on four key points, and they are:

Ability to eliminate the identify business problems: The s22 Pilot approach provides a sound model on which to address the business problems identified.

The s22 environment provides a suitable opportunity for the focus of the AusTender staff and management team to remain on the policy and strategic objectives of AusTender without the distraction of hardware acquisition.

The s22 model eliminates the need for AusTender team members to interact with hardware providers and the associated sourcing issues identified as an existing business problem.

The need for the AusTender application to operate with two separate providers, an application service provider and a hardware service provider, is eliminated under the s22 model. The existing application service provider is a partner s22 and therefore will allow AusTender to have a single point of accountability in terms of the AusTender technology service performance.

Value for Money: It is apparent from the outstanding ROI and NPV results that the existing cost structure that applies to the AusTender circumstances for hardware infrastructure services cannot continue. The traditional concept of hardware acquisition that involves the upfront investment in dedicated hardware that is specified to last for 4 years and to deal with the anticipated peak loads that will occur during that period cannot withstand the challenges brought on by the 'pay-as-you-go' model offered by the Cloud model.

Ease of Implementation: The s22 delivery model allows appropriately skilled and authorised administrators to provision the necessary hardware via a web-based user interface or via application programming interfaces (which means that a software program can give s22 systems instructions equivalent to those available via the web-based interface). This contrasts markedly with a typical acquisition and provisioning timeframe in traditional hardware arrangements requiring weeks. Indeed the proof-of-concept and the need in that process to develop a preliminary architecture using AusTender, has laid a good foundation for the work necessary to prepare for a comprehensive migration s22 that would serve the s22 Pilot well.

Opportunity to inform Australian Government agencies: Decision-makers across Australian Government agencies will be interested in the factors and considerations relevant to a migration to Cloud-based infrastructure. A comprehensive framework for considering those factors has been developed by central agencies, including extensive work by AGIMO, Attorney-General's Department and Australian Signals Directorate. A practical case study based on the AusTender experience would provide a further basis for agencies to understand the process and associated issues needing attention in such a migration. The development of such a case study will also provide practical information for individuals and groups within agencies that are interesting in building skills in this area. Importantly, the case study will also provide decision-makers in the Australian Government with a means of verifying the business benefits that are attributed to Cloud-based hosting, at least as far as the model shares similarities with the AusTender circumstances.

This recommendation does leave scope for the Department of Finance to approach the market at the conclusion of the Pilot. This is recommended, because it will ensure that the contract is contested in a local Australian market that currently has scope for additional maturity, which could be realised during the period of the Pilot.

4.5 Agency Capability

The Department of Finance, and specifically the AusTender team, maintains skills and expertise in accordance with its responsibilities.

These skills and expertise include Project Management, Contract Management and Service Management skills. Each of these is explained below and a maturity rating for each is provided.

Project Management

The assessment of Project Management Maturity is based on the organisation displaying attributes in the following areas as per the P3M3 model:

Management Control, including Project Management being seen as a key delivery mechanism;

Benefits Control, including approaches and processes that in relation to benefits measurement and realisation;

Financial Management, including established standards for the preparation of business cases and processes for their management throughout a project, prioritisation of investment against stated business goals;

Stakeholder Engagement, including analysis and communications planning for projects, a structured approach to engaging with stakeholders throughout the project;

Risk Management, including documented mechanism for identifying and management of project risk, ability to demonstrate resource and budgetary implications of risks throughout a project;

Organisational Governance, including reporting lines, accountabilities, responsibilities documented and understood, formalised decision making and decision review mechanisms, performance; and

Resource Management, including capability development strategies, policies and plans on improving capabilities, resource availability and capability profiling.

Levels of Maturity	Description of Maturity Level	AusTender Maturity Level
Level 1	Ad hoc	
Level 2	Repeatable	
Level 3	Defined	✓
Level 4	Managed	
Level 5	Optimised	

Contract Management

The maturity of Contract Management relates to all of the activities that are undertaken in the following areas:

Procurement Planning: The process of identifying which business needs can be best met by procuring products or services outside the organisation.

Solicitation Planning: The process of preparing the documents needed to support the solicitation.

Solicitation: The process through which a buyer requests bids, quotes, tenders, or proposals orally, in writing, or electronically.

Source Selection: The process by which the buyer evaluates offers, selects a seller, negotiates terms and conditions, and awards the contract.

Contract Administration: The process of ensuring compliance with contractual terms and conditions during contract performance up to contract closeout or termination.

Contract Closeout: The process of verifying that all administrative matters are concluded on a contract that is otherwise physically complete.

Levels of Maturity	Description of Maturity Level	AusTender Maturity Level
Level 1	Ad hoc	
Level 2	Basic	

Level 3	Structured	
Level 4	Integrated	✓
Level 5	Optimised	

Service Management

The AusTender team employs ITIL as its Service Management framework.

This framework includes the following areas: Service Desk

- Request Fulfilment
- Event Management
- Incident Management
- Problem Management
- Change Management
- Release Management
- Configuration Management
- Service Level Management
- Availability Management
- Capacity Management
- IT Service Continuity
- IT Financial Management

Levels of Maturity	Description of Maturity Level	AusTender Maturity Level
Level 1	Ad hoc	
Level 2	Repeatable	
Level 3	Defined	
Level 4	Managed	✓
Level 5	Optimised	

Aside from the skills identified above, the AusTender delivery model already includes the utilisation of external technology partners. The technical skills sets relevant to the transition to s22 environment will be the responsibility s22 the AusTender application technology service provider. s22 has been contributing to the success of AusTender since 2005. s22 led the most recent hardware refresh project for AusTender in 2012 and was integral to the project's success. The project delivered a new hardware architecture, a fully redundant system that met the imperatives for business continuity, disaster recovery and evolving security policy. The project also introduced a range of new technologies to support database replication and system/network management. s22 managed the solution design, project documentation, and the application layer build and implementation; they actively collaborated with the

hardware vendor and the secure hosting environment provider to foster goodwill, co-ordinate the work effort of all parties and ensure the project was delivered on time and budget.

s22 experienced in the utilisation of Cloud based infrastructure platforms. This experience extends to Cloud infrastructure arrangements for clients across a range of industries including media, entertainment, travel, hospitality and finance.

4.6 Security and information assurance

Data security has been an area of ongoing concern in relation to the adoption of Cloud-based services by Australian Government agencies.

In relation to the AusTenders22 Pilot, a comprehensive range of security controls will need to be employed, and each of these will be tested against the requirements of the relevant aspects of the Attorney-General's Protective Security Policy Framework and the Australian Signals Directorate's Information Security Manual.

A key security measure throughout the design, implementation and ongoing operation of thes22 Pilot will involve the engagement of an independent assessment of the security provisions in place by an ASD accredited IRAP assessor.

The following IRAP roadmap will be followed to ensure security through the design, implementation and ongoing operations:

1. Review this document and consider the recommendations; adopt the technical controls if feasible i.e. Anti-virus, host intrusions detection, host firewall
2. Review the non-technical control and adopt the recommendations where feasible i.e. ASD Cloud Security Considerations
3. Identify an AusTender IT Security Manager, document their role and ensure they are the main security contact for the agency
4. Engage a security professional to assist in the drafting of key security documents in accordance with government requirements; decide if the documents are to be drafted in-house under guidance or outsourced
5. Document the system design and record design decisions
6. Develop a Statement of Applicability to identify which parts of the ISM apply to the solution
7. Security risk assess the design
8. If necessary adjust the design in order to mitigate specific risks; update the design document
9. Create a Security Risk Management Plan to identify key security controls
10. Seek formal approval of the system architecture and compliance posture by the system owner
11. Create a System Security Plan
12. Create Standard Operating Procedures covering such topics as patching and administration tasks
13. Develop an Incident Response Plan and include procedures for the management of DDOS/DOS
14. Engage an IRAP Assessor to undertake a Stage 1 audit of the documentation

15. Build the system
16. Undertake vulnerability testing of the system and mitigate identified issues prior to commissioning
17. Engage an IRAP Assessor to undertake a Stage 2 audit of the as-built system
18. Seek accreditation of the system by the business owner and acceptance of residual risk
19. Operate the system in accordance with documented policy and procedures, ensuring the system in patched regularly
20. Undertake regular vulnerability assessment throughout the systems lifecycle
21. Reaccredit the system at regular intervals or as a result of significant system changes, and
22. Respond to incidents in accordance with the documented IRP and report incidents to ASD Cyber Security Operations Centre.

It is worth noting here that Australian Government position on offshore data storage, as defined in the *"Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements"* document, would require AusTender to gain Ministerial approval from the Minister for Finance and the Attorney-General prior to entering arrangements to hold personal information offshore. AusTender has no intention of making arrangements for AusTender data to be stored or processes offshore, and it is clearly understood that s22 able to accommodate the AusTender data storage arrangements using onshore facilities.

4.7 Risks

A number of generic risks have been identified as being worthy of consideration by the Australian Government when considering transition to the Cloud. These risks were published by Department of Finance in April 2013 in a document titled 'Cloud Computing Strategic Direction Paper v1.1'. The relevant risks are listed in the table below with AusTender-specific elaboration for each risk.

s47C

[redacted]

s47C [redacted]

Funding model	• Due to the Cloud's pay-per-use model, some part of ICT capital budgeting will need to be translated into operating expenses (OPEX), as opposed to capital expenditure (CAPEX), which may have different levels of authorisations to commit expenses and procure services.	• The cost models suggest a significant decrease in CAPEX requirements for AusTender. The cost modelling suggests a reduction in operating costs also. • The AusTender team will need to adjust their capital expense management plans to allow for these changes.
Legal and regulatory	• Need to have the ability to discover information under common law; • Need to be aware of Australian legislative and regulatory requirements including Archives Act, FOI Act and Privacy Act; • Need to be aware of data sovereignty requirements; • Need to be aware of legislative and regulatory requirements in other geographic regions, as compliance may be a challenge for agencies; and • Little legal precedent exists regarding liability in the Cloud and because of this, service agreements need to specify those areas the Cloud provider is responsible for.	• Ongoing access to AusTender application information and the data stored in relation to the application will need to be addressed in the agreement for hosting services. • Archives, FOI, and Privacy legislation requirements will be addressed at the time of formation for the hosting services. • The default s22 customer agreement is understood to be governed under the laws of the State of Washington, USA.

Performance and conformance	• Need to ensure that guaranteed service levels are achieved. This includes environments where multiple service providers are employed (e.g. combined agency and Cloud environments). Examples include:
	  ○ Instances of slower performance when delivered via internet technologies;
	  ○ Applications may require modification;
		• s22 past performance statistics suggest that the required levels of performance are achievable.
		• Application monitoring will be included as part of the design to ensure performance can be monitored and related issues addressed.

Issue	Explanation	AusTender Specific Considerations
	○ Monitoring and reporting are adequately delivered for the period between service introduction and exit; and ○ Failure of service provider to perform to agreed-upon service levels.	
Privacy	• Risk of compromise to confidential information through third party access to sensitive information. This can pose a significant threat to ensuring the protection of intellectual property (IP), and personal information. **Future privacy compliance** From March 2014, thirteen new Australian Privacy Principles (APPs) will apply to both the public and private sector. For Australian Government agencies these APPs will replace the current IPPs. The APPs are structured to reflect the information life cycle from notification and collection, through to use and disclosure, security, access and correction. With the changes to the Privacy Act in March 2014, agencies should start preparing now to ensure compliance with the new APPs. This may include considering the impact of the APPs in any Cloud computing procurements agencies anticipate undertaking. The OAIC will produce detailed guidance published on the OAIC website to assist agencies to understand the impact of the reforms and make the necessary changes to agency information handling practices.	• The nature of sensitive information that passes through AusTender makes its ongoing protection a priority. At an application level various controls are in place to encrypt sensitive data and prevent unauthorised access to this data. • The obligations under the new Privacy principles have been reviewed and no issues arise in relation to the planned hosting arrangements of AusTender.
Reputation	• Damage to an agency's reputation resulting from a privacy or security breach, or a failure to deliver an essential service because risk was inadequately addressed must be considered for Cloud computing applications.	• Both Finance and s22 have a very strong sense of the implications that a privacy or security breach would have on them. As a result a careful approach to application and data security with input from an independent IRAP assessor is planned.
Skills requirements	• A direct result of transitioning to a Cloud environment means: ○ Less demand for hardware and system management software product-specific skills; and ○ More demand for business analysts,	• The Finance AusTender team and their technology partners feel that the teams are adequately resourced to address the requirements of the recommended option.

Issue	Explanation	AusTender Specific Considerations
	architects, portfolio and program and change managers, and vendor/contract managers.	
Security	• Must ensure Cloud service providers and their service offerings meet the requirements of the Protective Security Policy Framework (PSPF), the Australian Government Information Security Manual (ISM) and the Privacy Act 1988; and • With Cloud computing, an agency may have limited ability to prescribe the protective security of the Cloud environment. Yet agencies will remain ultimately responsible for the information that is stored and/or processed in the Cloud. Management must maintain assurance that the security of the Cloud service provider is in accordance with the PSPF.	• IRAP assessment at the design, implementation and operational stages will provide a high degree of assurance on security
Service provision	• Reputation, history and sustainability should all be factors to consider when choosing a service provider; • Agencies should take into consideration the volatility of the growing Cloud computing market; and • Agencies should ensure they address portability of data in the case of service provider failure.	• A Pilot with s22 is recommended because of the independently sourced confirmation of their maturity and capability in delivering Cloud services.
Standards	Strategies for open standards, interoperability, data portability, and use of commercial off the shelf (COTS) products are required for reducing the risk of vendor lock-in and inadequate data portability. Examples include: • Potential for inadvertent use of Cloud services creating "islands" of Cloud technologies that will reduce interoperability across Cloud types and associated implementations; • A Cloud provider decides to no longer stay in business, an agency's data/application/processes must be able to be moved to another provider; and • Certification of projects by vendors for prescribed platforms and versions.	• The potential for lock-in and the means to avoid it will be a key consideration during the design stage of the migration of AusTender to the s22 environment. Initial assessments on this aspect indicate that Finance will be well placed to migrate to other Cloud environments without incurring prohibitive costs.

5. Implementation Strategy

The following section of the document sets out the expectations around how the recommended option from the business case will be managed as a formal project.

5.1 Governance Arrangements

It is proposed that the AusTender Cloud Migration project be overseen by a governance group, functioning in accordance with Prince2 project management methodology practices, with constituents possessing experience and knowledge relevant to the project and its objectives.

The project governance arrangements will ensure that the following aspects of the project are adequately considered or addressed from inception and throughout:

- Project funding
- Project staffing and accountability
- Project progress
- Project scope control
- Project benefits realisation
- Project risk management

5.2 Project Management Plan

The project management plan will consist of a number of component parts; each of these component parts is discussed below.

Scope Management

The development of the AusTender Cloud Migration project implementation scope will follow these steps:

- Decomposition of the entire project scope (as agreed with the Project Steering Committee) into a sensible hierarchy of work streams, and within these streams individual work packages will be identified and defined
- Work packages will be analysed and underlying tasks will be identified
- Tasks will be assessed and the estimated task duration established
- Tasks will be assessed and task dependencies (inputs) will be established.

Any changes to the scope during the course of the project will be subject to the project scope change management process.

Occasionally, approved changes to the project's scope may result in the schedule needing to be re-baselined. These scope changes may include new deliverables or requirements that were not previously considered as part of the original schedule's development. In these situations the project manager and team must consider the current status of the project schedule and how the scope change will affect the schedule and its resources as the project moves forward. How you handle scope change must be clearly documented in the Schedule Management Plan.

Any changes in the project scope, which have been approved by the Project Sponsor, will require the project team to evaluate the effect of the scope change on the current schedule. If the Project Manager determines that the scope change will significantly affect the current project schedule, he/she may request that the

schedule be re-baselined in consideration of any changes which need to be made as part of the new project scope. The Project Sponsor must review and approve this request before the schedule can be re-baselined.

Schedule Management

This section provides a general framework for the approach which will be taken to create the project schedule. This includes the scheduling tool/format, schedule milestones, and schedule development roles and responsibilities.

The project schedule will be reviewed and updated as necessary on a bi-weekly basis with actual start, actual finish, and completion percentages which will be provided by task owners.

The Project Manager is responsible for holding bi-weekly schedule updates/reviews; determining impacts of schedule variances; submitting schedule change requests; and reporting schedule status in accordance with the project's communications plan.

The project team is responsible for participating in bi-weekly schedule updates/reviews; communicating any changes to actual start/finish dates to the Project Manager; and participating in schedule variance resolution activities as needed.

The Project Sponsor will maintain awareness of the project schedule status and review/approve any schedule change requests submitted by the Project Manager.

If any member of the project team determines that a change to the schedule is necessary, the Project Manager and team will meet to review and evaluate the change. The Project Manager and project team must determine which tasks will be impacted, variance as a result of the potential change, and any alternatives or variance resolution activities they may employ to see how they would affect the scope, schedule, and resources. If, after this evaluation is complete, the Project Manager determines that any change will exceed the established boundary conditions, then a schedule change request must be submitted.

Submittal of a schedule change request to the project sponsor for approval is required if either of the two following conditions is true:

The proposed change is estimated to reduce the duration of an individual work package by 10% or more, or increase the duration of an individual work package by 10% or more.

The change is estimated to reduce the duration of the overall baseline schedule by 10% or more, or increase the duration of the overall baseline schedule by 10% or more.

Any change requests that do not meet these thresholds may be submitted to the Project Manager for approval.

Once the change request has been reviewed and approved the Project Manager is responsible for adjusting the schedule and communicating all changes and impacts to the project team, project sponsor, and stakeholders. The Project Manager must also ensure that all change requests are archived in the project records repository.

Note that a preliminary draft project schedule has been prepared and included at the end of this document in Appendix 2.

Cost Management

The Project Manager will be responsible for managing and reporting on the project's cost throughout the duration of the project. During the monthly project status meeting, the Project Manager will meet with management to present and review the project's cost performance for the preceding month. Performance will be measured using earned value. The Project Manager is responsible for accounting for cost deviations and presenting the Project Sponsor with options for getting the project back on budget. The Project Sponsor has the authority to make changes to the project to bring it back within budget.

The Cost Management Plan clearly defines how the costs on a project will be managed throughout the project's lifecycle. It sets the format and standards by which the project costs are measured, reported and controlled. The Cost Management Plan identifies:

- Who is responsible for managing costs
- Who has the authority to approve changes to the project or its budget
- How cost performance is quantitatively measured and reported upon, and
- Report formats, frequency and to whom they are presented.

Quality Management

The Quality Management Plan for the AusTender Cloud Migration Project will establish the activities, processes, and procedures for ensuring a quality product upon the conclusion of the project. The purpose of this plan is to:

- Ensure quality is planned
- Define how quality will be managed
- Define quality assurance activities
- Define quality control activities, and
- Define acceptable quality standards.

The explicit activities that are expected to be necessary to assure quality are:

- Establish a Management Reporting Structure and Status Reporting schedule
- Conduct an Environmental Analysis to define current environment capacity / performance, SLA / KPI / Contract requirements, gaps and exceptions, and obstacles that prevent achieving project goals
- Creation of an Applications Migration Project Plan with tasks to be performed, subject matter experts, deliverable time schedule, resource requirements, tasks to be performed, and costs
- Identify target environment and automated tools needed to help achieve project goals
- Define an Organization Structure for application migration, data centre decommission, and testing of production and recovery procedures
- Formulate Migration Path to move applications from existing data centre to target Cloud environment, with personnel functional responsibilities, job descriptions, standards and procedures, and training to all personnel assigned to this project
- Implement Migration Factory and other functional areas needed to perform migration duties
- Benchmark applications and systems at primary site and target site, reporting results to management
- Undertake series of application level tests, as agreed, likely including:
    - Service Form and Results Assessments

  - Application Group Testing Results
  - Test Scenarios and Scripts
  - s22 Messages and Codes, and Recoveries
  - Data for Regression and Normal Testing, and
  - Documentation
- Implement SDLC, Systems Management, Version and Release Management, and ITIL to support and maintain production operations going forward; integrate within everyday functions to ensure currency.

HR Management

Human resources management is an important part of the Upgrade Project. The Human Resources Management Plan is a tool which will aid in the management of this project's human resource activities throughout the project until closure. The Plan includes:

- Roles and Responsibilities of team members throughout the project
- Project Organization Charts
- Staffing Management Plan, to include:
  - How resources will be acquired
  - Timeline for resources/skill sets, and
  - Training required to develop skills.

The purpose of the human resources management plan is to achieve project success by ensuring the appropriate human resources are acquired with the necessary skills, resources are trained if any gaps in skills are identified, team building strategies are clearly defined, and team activities are effectively managed.

The project will employ a RACI (responsible, accountable, consult, inform) responsibility assignment matrix (RAM). This RACI RAM will provide a graphic display of the project tasks and team members. The purpose of this is to illustrate the responsibilities of team members as they relate to the project tasks.

Communications Management

Communications planning involves planning for all the communications with project stakeholders. The AusTender Cloud Migration project will employ a reporting schedule that identifies all of the audience groups; for each audience group the project team will identify their reporting needs. Once those reporting needs are determined then the most appropriate format and frequency of communication with that group can be established. These elements should then be reflected in the RACI RAM mentioned above under Scope Management.

Stakeholder	Reporting needs	Format	Preferred medium	When	Person responsible
Sponsor	Status report - including schedule, budget, variances, issues	Spreadsheet for schedule and budget status, table for scope status and issues plus a one page summary	Email attach. 24 hours prior to face to face meeting	Meeting last Mon. of each month prior to Board meeting	Project Manager

Communication protocols include:

- Communication method
- Standards
- Templates
- Security
- Ethics
- Time-frames and reporting schedules
- Who requires the information, and
- Version control method.

Risk Management

NB: It is noted here that Finance has a robust risk management framework that is to be uniformly applicable to activities occurring within Finance. That framework was not fully implemented at the time of this document being prepared, however it is expected to be in place by the time the AusTender Cloud Migration project is undertaken. Accordingly, the Finance risk management framework and the tools within it are expected to be adopted for this project.

Management Framework

Risk management assists the delivery of quality products on-time, on-budget and without avoidable business risk. A risk is an uncertain event or condition with a positive or negative effect on the project objectives and risk management addresses the events with adverse project impacts. Successful risk management pre-empts and mitigates risks rather than reacting to events which have already impacted the initiative.

Risk Management Plan

The Risk Management Plan covers the overall approach to risk management and defines the resources and tools that will be used to identify, log and manage risks to the project.

Risk Identification and Assessment

Risk identification is the process of identifying and classifying risks. Risk assessment covers the review and prioritisation discipline that will be used to assess all risks identified. The risk identification and assessments are recorded in the Risk Register.

Risk Response Planning

Risk Response Planning defines how each project will manage the risk. The risk response describes the project strategy to manage the risk. Responses can range from passive acceptance of risk outcomes through active mitigation. The risk response is recorded in the Risk Register.

Risk Monitoring and Control

Project risks will be documented in a Risk Register as part of Project Initiation. The Risk Register is based on the Risk Assessment Worksheet from the Commerce Intranet.

Maintaining and communicating the Risk Register is a core Project Manager responsibility.

Assessing the Risk

The following table indicates degree of likelihood - the probabilities that identified threats will occur - with associated ratings.

Risk Likelihood Ranking Table

Rating	Assessment Criteria	Probability
Very unlikely	The event may occur in exceptional circumstances	<21%
Unlikely	The event could occur at some time	21-40%
Medium	The event will probably occur at some time	41-60%
Likely	The event will probably occur in most circumstances	61-80%
Almost certain	The event is expected to occur in most circumstances	>80%

The following table indicates levels of impact - the specific damage or consequences to the project if identified threats occur - with associated ratings.

Risk Impact Ranking Table

Rating	Assessment Criteria	Probability
Very low	The event will cause little disruption	<21%
Low	The event will cause minor delay, reworking or rescheduling	21-40%
Medium	The event will cause a significant loss of time or money	41-60%
High	The event will cause major disruption or dislocation	61-80%
Critical	The event will more than likely cause the project to stop	>80%

By combining the Likelihood and the Impact, the following risk assessment matrix can be used to provide an overall risk rating.

Consolidated Risk Rating Table

Likelihood / Impact	Very Unlikely	Unlikely	Medium	Likely	Almost Certain
Very Low	1	2	3	4	5
Low	2	4	6	8	10
Medium	3	6	9	12	15
High	4	8	12	16	20
Critical	5	10	15	20	25

The following table explains the legend used in the risk analysis matrix above:

Risk Rating Legend

Risk	Required Actions
Very High Risk	Significant Risk – Immediate treatment required.
High Risk	Significant Risk – Treatment required as high priority.
Moderate Risk	Accepted Risk – Manage by specific monitoring or response procedures, with management responsibility specified and strategies implemented as part of day-to-day project management.
Low Risk	Rejected Risk – Manage and monitor by routine internal procedures.

Procurement Management

The Procurement Management Plan should be defined enough to clearly identify the necessary steps and responsibilities for procurement from the beginning to the end of a project. The Project Manager must ensure that the plan facilitates the successful completion of the project and does not become an overwhelming task in itself to manage. The Project Manager will work with the project team, contracts/purchasing department, and other key players to manage the procurement activities. The Business Project Manager will provide oversight and management for all procurement activities under this project.

Benefits Realisation Strategy

Benefits Management is a business function under the direction of the Project Sponsor.

The ongoing management of business benefits demonstrates the linkages between ICT investments, Government policy priorities, Finance business objectives and service delivery outcomes. It includes the management processes and accountabilities being used to ensure that benefits claimed for a project are tracked and achieved over the entire project lifecycle.

The outcomes of this project are aligned to broader policy directions outlined in the Australian Government ICT Strategy 2012-2015. The ICT Strategy framework and this project business case provides an opportunity for measuring and monitoring performance management framework that could be leveraged to capture benefits flowing from this project and other comparable initiatives. An ongoing analysis of the benefits attributable to AusTender more broadly is maintained by the Department of Finance.

Stakeholder Management

The stakeholder consultation strategy for the AusTender Cloud Migration Project as it relates to Government entities will be based largely on continued engagement with the constituent members of the Australian Government AusTender Agency Reference Committee, along with engagement at key points in the process with central government bodies including the Australian Government Information Management Office and Australian Signals Directorate.

Industry and more particularly the AusTender registered user-base consultation will require the establishment of a carefully structured awareness and engagement framework to cater for any possible disruptive activities throughout the migration. The nature of the project should not be noticeable to stakeholders apart from the knowledge that they should experience fewer planned service outages and faster response times once migration to the new environment is complete.

As mentioned above, the development of a case study reflecting the considerations and outcomes of this project will provide an avenue for further engagement with a broader set of stakeholders across the Australian Government. As the case develops an engagement and distribution model will be developed.

6. Appendices

Appendix 1: Business Case Information and Research Sources:

- ANAO Audit Report No.44 2008–09 Security Risk Management
- Cloud Leadership Forum Governance Frameworks
- AGIMO A Guide To Implementing Cloud Services
- Australian Public Sector ICT Strategy 2012 to 2015
- Australian Government Classification System
- Australian Government Cloud Computing Policy Version
- Australian Government Architecture Framework Principles
- Australian Government Cloud Computing Strategic Direction Paper - Opportunities and applicability for use by the Australian Government – April 2013
- s22 [redacted]
- Case for Cloud Computing –s22 [redacted]
- CIO Magazine How to Migrate Enterprise Apps To Cloud
- European Network and Information Security Agency - Cloud Computing Security Risk Assessment
- USA Government– Cloud Migration Services Statement of Objectives
- Department of Defence – Cloud Computing Security Considerations
- American Internet Services - Cost and risk in assessing Cloud value

s22 [redacted]

- Coalitions Policy for E-Government and the Digital Economy
- Defining Cloud Computing in Business Perspective: A Review of Research
- Storage Network Industry Association - Building the Business Case for the Cloud

s22 [redacted]

- Computer Weekly Sept 2013 – "Public sector IT procurement, G-Cloud and the small guys".
- http://www.liberal.org.au/boosting-productivity-and-reducing-regulation
- IDC: The Business Value of Amazon Web Services Accelerates Over Time - July 2012
- A report for the Secretary of the Commonwealth Department of Finance and Deregulation on the draft ICT Strategic Vision
- KPMG: Exploring the Cloud
- AGIMO: Negotiating the Cloud – Legal Issues In Cloud Computing Agreements - Better Practice Guide
- Australian Government Policy and Risk management guidelines for the storage and processing of Australian Government information in outsourced or offshore ICT arrangements
- Productivity Commission Research Paper: ICT Use and Productivity: A Synthesis from Studies of Australian Firms
- Independent Review of Implementation of the ICT Reform Program - Dr Ian Reinecke June 2010
- Designing Private and Hybrid Clouds - s22 [redacted]
- 7 Key Drivers For Cloud Migration: Transformational Metrics and analytics for Managing 'Infrastructure Anywhere': Sentilla

s22

- AGIMO Cloud Financial Better Practice Guide
- Department of Finance and Deregulation P3M3 Assessment Report
- Department of Finance Guidance on the Assurance Reviews Process – Sept 2013
- Department of Finance ICT Two Pass 2nd Pass Business Case Template
- Department of Finance ICT Two Pass Presentation
- Outsourcing Digital Data Storage – National Archives of Australia
- Records Management And The Cloud – National Archives of Australia

Appendix 2: Preliminary AusTender Cloud Migration Schedule

Dates / Activities	March				April				May				June				July				August				September			
	Wk1	Wk2	Wk3	Wk4	Wk5	Wk6	Wk7	Wk8	Wk9	Wk 10	Wk 11	Wk 12	Wk 13	Wk 14	Wk 15	Wk 16	Wk 17	Wk 18	Wk 19	Wk 20	Wk 21	Wk 22	Wk 23	Wk 24	Wk 25	Wk 26	Wk 27	Wk 28
Business Case																												
Project Initiation																												
Project Scoping																												
Solution Design																												
IRAP Assessment Post-Design																												
Solution Build																												
IRAP Assessment Post-Build																												
Solution Testing																												
Deployment																												

As can be seen from the preliminary project schedule above the recommended Option 2 s22 Pilot does have sufficient time prior to the term of the existing arrangements with s22 concluding on 27th September 2014. This schedule has intentionally made use of that time with an extended testing and quality assurance

period. Other activities that should be included in that period include the preparation for disposal of retired equipment, and post-implementation service management planning and procedures.