Australian Government

Department of Finance and Deregulation
Australian Government Information Management Office

A Guide to Implementing Cloud Services

Better Practice Guide

SEPTEMBER 2012

AGIMO is part of the Department of Finance and Deregulation

Disclaimer

This document has been prepared by AGIMO in consultation with other agencies to provide an overarching risk-managed approach for agencies to develop an organisational cloud strategy and implement cloud-based services.

This document and the information contained herein are provided on an "as is" basis and the contributors and the organisations they represent and are sponsored by disclaim all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

Links to other websites are inserted for convenience only and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

AGIMO is part of the Department of Finance and Deregulation

Contents

1. Introduction

The Australian Government's policy on cloud computing is that agencies may choose to use cloud computing services where they provide value for money and adequate security, as stated in the April 2011 *Australian Government Cloud Computing Strategic Direction Paper*[1] (the *Strategic Direction Paper*).

Readers new to cloud computing should read the Strategic Direction Paper which provides an introduction to cloud computing, a definition and an overview of its associated risks and benefits as they apply to Australian Government agencies.

The guide supports the *Strategic Direction Paper* and provides an overarching risk-based approach for agencies to develop an organisational cloud strategy and implement cloud-based services. It is designed as an aid for experienced business strategists, architects, project managers, business analysts and IT staff to realise the benefits of cloud computing technology while managing risks.

Agencies should use this guide to understand the issues surrounding moving services to the cloud. It focuses on activities to identify and implement cloud opportunities, and points to the following better practice guides where appropriate:

1. Defence Signals Directorate's *Cloud Computing Security Considerations*[2];
2. National Archives of Australia's *Records Management in the Cloud*[3];
3. AGIMO's *Privacy and Cloud Computing for Australian Government Agencies*[1];
4. AGIMO's *Negotiating the cloud – legal issues in cloud computing agreements*[1];
5. AGIMO's *Financial Considerations for Government Use of Cloud Computing*[1]; and
6. AGIMO's *Community Cloud Governance – An Australian Government perspective*[1].

The guide contains the following major sections:

Section 2 outlines consideration for agencies to identify opportunities to benefit from cloud-based services, which they can incorporate into their ICT strategy. The following key areas are covered: suitability to business needs, timing and triggers, financial impacts, organisational capability and governance.

Section 3 provides implementation guidance across the lifecycle of a cloud solution project. The section addresses business analysis, risk management, business case development, procurement, solution implementation and transition to operation.

Section 4 provides a short list of post-implementation activities for agencies to consider.

Attachments include a checklist which follows the layout of this guide and a business case template for cloud solutions.

[1] http://www.finance.gov.au/e-government/strategy-and-governance/cloud-computing.html

[2] http://www.dsd.gov.au/infosec/cloudsecurity.htm

[3] http://www.naa.gov.au/records-management/agency/secure-and-store/rm-and-the-cloud

2. Identifying cloud opportunities

The *Strategic Direction Paper* provides high-level direction for using cloud-based services across the Australian Government. It also highlights the many benefits to be offered by cloud-based services, such as increased scalability, flexibility, availability and productivity. While cloud-based services share similarities with other service delivery models, e.g. managed services, they also offer their own unique opportunities, complexities and risks.

A coordinated approach between business and ICT managers is needed to identify opportunities to benefit from cloud-based services. The approach taken includes the following considerations:

- benefiting from other agency or whole-of-government cloud initiatives;
- alignment with the agency's business, ICT and information security strategy and policies;
- timing and triggers, such as planned system replacements or emerging business requirements;
- impacts on capital and operational expenditure;
- the ease with which staff members can sign-up and use cloud-based services, e.g. free basic services, without the requisite approvals or controls;
- the Australian Government's strategic direction on cloud computing and open government (Gov 2.0)[4];
- the complexity of integrating cloud-based services with existing processes and technology; and
- the risks associated with storing and processing information in the cloud, e.g. security and service provision lock-in.

Like any new delivery model, a first step is to target low risk, low value applications or pilots from which the organisation can measure actual costs and benefits, gain insights and draw lessons for future endeavours. The Strategic Direction Paper encourages agencies to adopt public cloud-based services for public facing "unclassified" government services and to undertake proof of concept studies to fully understand the risks of cloud computing.

Agencies should develop a coordinated approach to cloud-based services as an integral component of their ICT strategy and roadmap. Figure 1 shows the various inputs which agencies should consider as they develop such an approach. The following subsections offer guidance for each input area and point to details in the suite of better practice guides[1] where appropriate.

[4] http://www.finance.gov.au/e-government/strategy-and-governance/gov2.html

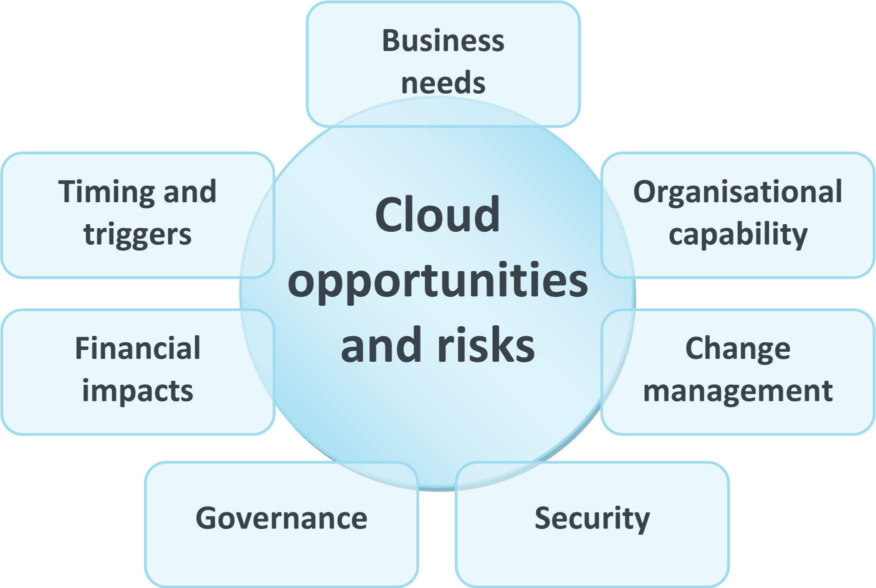

Figure 1. Inputs to a cloud approach

Support is available through the Cloud Information Community (CLIC), hosted by AGIMO. The CLIC serves to help agencies stay informed with developments in cloud policy and cloud-based services being used by other agencies. AGIMO strongly encourages agencies to provide details of cloud-based services and lessons learned to the CLIC so that other agencies can factor these into their strategy and implementation programs.

Agencies should also notify AGIMO at architecture@finance.gov.au when considering cloud-based services, per *AGIMO Circular 2011/001*[1] to help identify solutions that may contribute to whole-of-government initiatives.

2.1 Assess suitability against business needs

Agencies should identify the information types, services and associated business processes which stand to gain the most from cloud-based services and assess the impact of moving them to the cloud. The agency's enterprise architecture will provide a useful place to start this analysis.

2.1.1 Information

From an information perspective, agencies maintain the same legislative and policy obligation to protect and manage information across the information lifecycle regardless of where it is stored and processed. Such obligation includes compliance with the *Protective Security Policy Framework (PSPF)*[5] and the *Information Security Manual (ISM)*[6]. Agencies should take an information security management approach to determine which information sets to transition to cloud-based services. This includes assessing the business impact(s) that could result from the compromise, loss of, or disruption of access to information. The assessment should include the risk posed by data that has been aggregated. The *Protective Security Governance*

[5] http://www.protectivesecurity.gov.au/

[6] http://www.dsd.gov.au/infosec/ism/

Guidelines - Business Impact Levels[7] provides a common tool to assist agencies to assess the business impact for compromises of confidentiality, integrity or availability of individual or aggregated information, ICT systems and other assets.

To assess the types and classifications of information that will best benefit from cloud-based services, agencies should consider the following factors across the information lifecycle:

- potential adverse impact to the reputation of the Australian Government;
- potential impact to the governance of information, with particular reference to ownership, stewardship and custodianship responsibilities;
- potential impact to an agency's ability to develop flexible business processes that span one or more cloud-hosted solutions and possibly in-house hosted systems;
- potential impact to agency business processes if a business service or an IT services is transitioned to a cloud solution;
- potential impact to business continuity should a cloud solution no longer be available.
- ability to assure the availability, integrity and confidentiality of information (refer to *Cloud Computing Security Considerations* and *Privacy and Cloud Computing*);
- potential impact to data formats and interoperability;
- impact on existing architecture and integration with existing systems;
- potential impact to data access, discovery, archival and destruction;
- the ability of the agency to maintain legislative and regulatory compliance, e.g. with the *Archives Act 1983* (refer to *Records Management in the Cloud*); and
- the cloud deployment model (i.e. public, private, community, hybrid) that would be most appropriate.

2.1.2 Services

As part of determining which services are appropriate for the cloud, agencies should consider the business problem or opportunity. When evaluating which end-to-end business services are suitable for the cloud, agencies should consider the services that:

- have stable and consistent functional requirements;
- could be readily shared with other agencies with similar needs;
- have cyclical, seasonal or uncertain demand, and could benefit from added flexibility from the cloud;
- aren't highly integrated with in-house applications or other processes;
- have data formats or portability requirements that are not critical;
- have manageable business continuity requirements;
- have discrete components of the end-to-end business process that can be transitioned to the cloud, e.g. public-facing workflows; and
- have functional requirements that could be met by cloud-based services.

[7] http://www.protectivesecurity.gov.au/governance/security-risk-management/Pages/Supporting-guidelines-for-security-risk-management.aspx

With an understanding of which information, services and business processes that would benefit most from cloud-based services, agencies should assess the technical barriers they will have to address. Factors such as impacts to existing infrastructure, e.g. bandwidth, and enterprise applications apply to even the simplest cloud-based services. Hybrid cloud-based services that integrate with in-house software services will require an in-depth investigation into technical issues such as service orchestration, programming interfaces, data format standards and latency.

2.2 Consider timing and triggers

An agency's architectural roadmap and project portfolio will provide useful tools to identify the timing and trigger points that present opportunities for the use of cloud-based services. Agencies should consider:

- business and IT systems scheduled for replacement;
- planned system implementations/upgrades;
- requirements for system development/testing where cloud infrastructure could be used;
- pilots, time-bound or short lifespan projects; and
- capabilities used only periodically.

Agencies should also seek opportunities to develop/adopt cross-agency or portfolio cloud-based services and/or build on initiatives established by other agencies. AGIMO provides assistance to agencies in finding shared resource solutions and can be contacted at architecture@finance.gov.au.

2.3 Consider financial impacts

The transition to cloud-based services will have financial and budgetary impacts that agencies must consider at strategic and operational levels. While cloud-based services have the potential to reduce capital expenditure, agencies will have to consider the impacts on their budgets and financial statements.

Any impacts will need to be reflected in the agency's financial statements. Any reduction in capital spending will need to be reflected in the agency's capital management plan. Refer to *Financial Considerations for Government Use of Cloud Computing* for more detailed coverage of this topic.

2.4 Consider organisational capability

The management of cloud-based services requires capabilities similar to that used in typical outsourcing arrangements. That is, agencies will require well-developed skills in project and program management, relationship management, procurement and contract management, and services provisioning and management. Agencies will also need to understand workflow design, cloud architecture and capacity management. Agencies that do not have mature capability in these areas should take a gradual approach to moving to cloud-based services while they develop that maturity. For example, a lack of service management maturity may lead to challenges for the management of service and performance, as with any outsourced arrangement.

Cloud-based services may require new skills. There may be a decreased need for specialist operation and support skills depending on the nature of the cloud solution, but there will also be a need for additional contract management capabilities.

The agency should also have mature capabilities in the areas of enterprise architecture and business analysis to assess and manage changes to its architecture and business processes. A cloud solution will not fix immature business processes or cultural issues.

Agencies should consider the strategic impact that their approach to cloud-based services will have on their organisation structure and skills sets, and implement a plan to mature capabilities in targeted areas.

2.5 Manage change

Agencies can improve the likelihood of successful adoption and user take-up of cloud-based services by actively keeping stakeholders informed and addressing their concerns. Stakeholder concerns may include:

- storing information in the cloud;
- uncertainty with new technology;
- shifting staff roles;
- increased dependence on a third party;
- the possibility of deterioration of customer care or service quality; and
- loss of control.

Agencies should establish a stakeholder engagement plan, obtain senior executive sponsorship and work closely with key stakeholders to ensure they are kept informed throughout.

2.6 Review governance

Well-defined, effective governance is essential for cloud computing. Agencies should review their governance model to ensure the structure, guidance and controls are adequate. Agencies should consider new or changed roles and responsibilities, such as the addition of CSPs and partner agencies for community clouds.

In the case of community clouds, the lead agency may need to review existing memorandums of understanding and establish a cloud computing agreement. The Better Practice Guide: *Community Cloud Governance – An Australian Government perspective* provides specific guidance on developing governance for community clouds and includes a sample governance structure. The information provided in this guide may translate to other cloud models.

3. Implementing a cloud solution

Implementation activities for a cloud solution are similar to that of an outsourced solution. That is, the agency will have to conduct business analysis, build a business case, source a cloud service provider (CSP), plan and implement the solution, possibly with the assistance of a third-party system integrator. This section provides advice across the lifecycle of a cloud solution project with the aim of ensuring the cloud solution will:

- meet business needs in terms of both functionality and performance;
- provide the expected efficiencies and benefits;
- adequately protect agency information;
- comply with legislative and regulatory requirements; and
- integrate with existing processes and systems.

3.1 Build a business model

The work to develop an agency's approach to cloud-based services will provide the business context required for candidate cloud-based services. Business analysis activities will be similar to those used for an outsourced solution. Such activities include building a business model and gathering requirements to form the basis for the business case, sourcing, implementation and testing.

The business model will help the agency determine performance and resource requirements, lifecycle cost estimation, and required risk treatment measures. Agencies should consider how they would respond to business continuity and disaster recover scenarios, such as cloud service disruption or cancellation. These scenarios can later be developed into requirements and plans.

The *Australian Government Architecture Reference Models*[8], in particular the Performance Reference Model, can be used to identify and define measures to quantify resource utilisation, costs attributed to business process execution and costs to promote the use of output by customers.

The business model must have sufficient detail to estimate cost in terms which can be applied to the CSP's cost model. For infrastructure as a service (IaaS) and platform as a service (PaaS), this might be measured in resource usage per period of time, as for processing, throughput and storage. For software as a service (SaaS), service might be measured by number of transactions or number of users.

With an understanding of which resources to measure, business analysts should model expected utilisation and potential surge scenarios by considering:

- user characteristics, e.g. user types/roles, number of users, usage scenarios;
- data characteristics, e.g. data types, size and quantity;

[8] http://www.finance.gov.au/e-government/strategy-and-governance/australian-government-architecture.html

- average usage rates, e.g. transactions per second
- how usage rates will vary, e.g. upper and lower ranges;
- where can changes to usage rates be predicted, either at planned times or based on events;
- how usage will grow or scale over time, perhaps with the number of users; and
- how usage will change for each system actor, e.g. end user, administrator, batch processes.

Where possible, agencies should validate the model either by comparison to existing systems, with a benchmarking program, or by piloting a solution. Cloud-based services may provide better value for short-term or burst use, but a non-cloud solution may provide more value over the long term, particularly for services with steady loads.

3.2 Assess the risks

Agencies should use the business model to undertake an initial threat and risk assessment (TRA). The PSPF states that agencies must apply a principles and risk-based approach to all areas of protective security activity across their organisation including service provider selection, in accordance with:

- AS/NZS ISO 31000:2009 – Risk Management, Principles and Guidelines; and
- HB 167:2006 Security Risk Management.

The other cloud computing better practice guides are a useful resource for agencies to help identify risks and determine suitable treatment strategies. Agencies should also consider the cost to manage the associated risks and its impact on the value proposition.

The following risk categories provide a useful start for identifying risks:

- Quality – does the cloud solution meet stakeholder needs;
- Financial – does the cloud solution provide value for money;
- Organisational – does the cloud solution work within the agency's culture;
- Integration – can the cloud solution meet objectives without business or technical integration difficulties;
- Compliance – does the cloud solution comply with agency's legal, regulatory and policy obligations;
- Business Continuity – can the cloud solution recover from outages or disaster situation; and
- External – is the CSP performance adequate.

3.3 Capture requirements

The business model and risk assessment provide a basis for determining requirements. For each requirement, agencies should note which are mandatory and which are desirable. It may be useful for agencies to use a standard practice description, such as the IT Infrastructure Library (ITIL), to ensure coverage of requirements which relate to the management of services.

3.3.1 Functionality

Functional requirements will differ according to the type of cloud service model:

- For IaaS, requirements will relate to the provision of processing, memory, storage and operating systems. Agencies will need to consider:
  - whether operating systems licence costs will be included in the solution or provided by the agency, and
  - what open source options are available.
- For PaaS, requirements should specify both the development and operating environment.
- For SaaS, requirements will be similar to those of a non-cloud solution.

Functional requirements should consider the ability to backup and restore data or system images, whether it is the provider's responsibility, and where backups will be stored. They should also consider any bulk data transfer, either as a part of normal operation or as part of an exit strategy. Agencies should consider the options available to transfer data, including network or physical transfers, such as tape or disc packs.

Lastly, agencies should consider any requirements to interoperate and/or integrate with in-house or back office systems, for example identity management and authentication systems.

3.3.2 Standards

Agencies will best achieve interoperability through the use of industry-recognised open standards. While cloud-based services are not a new technology, existing technology standards, programming interface standards and data formats may need to be amended and new standards implemented where necessary. For example, standards for configuration and management of cloud-based services are still maturing and tend to vary among CSPs.

Standards for cloud computing are evolving locally through the work of Standards Australia and the national mirror committee of international working group SC 38, a subcommittee of the ISO/IEC Joint Technical Committee 1. Agencies should monitor the development of international standards and adopt and apply them when available.

Agencies will need to ensure that the appropriate levels of security, interoperability, and data portability are factored into any architectural design work and into any contractual arrangements. Conformance to standards must also be tested during the implementation of a cloud solution.

3.3.3 Performance

Performance requirements derive from the business model and from business impact analysis. Although business will measure performance from the user's perspective, there are several factors such as client-side processing and network delays which CSPs will be unable to control.

Performance requirements, such as availability, reliability, recoverability, responsiveness and throughput are generally the same as for internal systems. Specific requirements to consider include:

- availability metrics include a unit of time, e.g. downtime per month;
- guaranteed maximum outages and outage durations if reliability is critical;

- how much data can be lost and the minimum acceptable time to recover from both transient and catastrophic failures;
- both average and peak response times for various types of transactions; and
- the data size for transactions, and peaks and averages from the usage model.

During procurement, agencies should define performance requirements and negotiate performance guarantees in contract. Refer to Section 3.6 *Define contractual terms* and Section 3.8 *Select a provider* for more details.

3.3.4 Manageability

There are several requirements to consider regarding the ability to configure and manage cloud-based services.

Agencies should note that the *ICT Customisation and Bespoke Development Policy*[9] applies to cloud-based services, particularly SaaS and PaaS where customisation may reduce the financial benefit for the agency.

Agencies should consider the following requirements:

- the ability to provision resources (e.g. on-demand or self-service), the speed of provisioning and the ability to cap resources;
- the availability of reports that map to business objectives and provide objective measurement of business performance, e.g. billed resources, resource utilisation, throughput, availability and any other quality of service measures;
- the frequency, format and delivery of reports; and
- the ability to manage faults, including procedures to report and check on faults, reporting channels, and availability of support staff.

CSPs will have differing service levels and capabilities to meet manageability requirements. Agencies should confirm that the CSP will have the ability to meet its requirements during the selection process.

3.3.5 Security

Security is a compulsory obligation as outlined in the PSPF and the ISM. Agencies must determine the level of security required by undertaking a risk assessment to determine the business impact for each information set that is being considered for transition to a cloud solution. The security assessment should consider:

- authorisation, end-user access controls and provider access controls;
- authentication, encryption, key management;
- data location and the applicability of foreign laws, data separation/segregation, data destruction;
- logging and audit;
- threat management; and
- physical security.

DSD has recommended that agencies undertake their risk assessments integrating the controls outlined in the *Cloud Computing Security Considerations*.

[9] http://www.finance.gov.au/e-government/strategy-and-governance/Whole-of-Government-ICT-Policies.html

3.3.6 Compliance

Agencies should keep in mind their legislative and regulatory obligations to keep data confidential or guarantee it's not lost or destroyed. Many of these will translate into specific security and requirements, or perhaps certification requirements.

Key legislation includes *Public Service Act 1999*, *Freedom of Information Act 1982*, *Privacy Act 1988*, *Archives Act 1983*, *Evidence Act 1995*, *Copyright Act 1968* and the *Electronic Transactions Act 1999*.

There may be other policies, strategies and frameworks that a CSP will need to comply with. Examples include:

- The Australian Government's Department of Finance and Deregulation circulars and advice including whole of government ICT policies, strategies, frameworks and policies, for example, use of Internet-based Network Connections Service (IBNCS) panel for all wide area network and internet connections, internet gateway reduction program for all internet gateways;
- agency-specific procurement policies; and
- agency-specific security policies.

Refer to *Privacy and Cloud Computing for Australian Government Agencies*, *Cloud Computing Security Considerations* and *Records Management in the Cloud* for further guidance.

3.4 Build a business case

A sound business case provides an objective view of the business rationale, benefits, costs, risks and options involved with solving a business problem. It provides the justification for a cloud solution weighed against other alternatives, such as non-cloud solutions. It also provides the basis for planning and implementing the solution. The business case justifies the appropriateness of the cloud solution and provides a reference point for re-evaluation at a future point in time, e.g. for changes to business requirements or emergence of new solutions in the marketplace.

AGIMO provides an ICT Business Case Guide, templates and costing spreadsheet which are required as part of the ICT Two Pass Review process[10] for ICT-enabled proposals with:

- high risks in terms of technical complexity, workforce or schedule, and
- a total cost of $30 million, including an ICT cost of $10 million or more.

For smaller initiatives, this guide provides a tailored version of the ICT Business Case Template as an attachment. The attachment provides specific guidance for developing a business case where a cloud solution is an option.

This section should also be read in conjunction with the *Financial Considerations for Government Use of Cloud Computing* which provides further advice on assessing financial risks and preparing a financial assessment.

The business case should begin with the rationale for adopting a cloud solution weighed against other alternatives. It should capture the business need, how the proposed adoption of a cloud computing solution meets that need, and how it aligns

[10] http://www.finance.gov.au/budget/ict-investment-framework/two-pass-review.html

with the agency's sourcing strategy and architecture. Where this involves a move away from traditional investments in ICT infrastructure and to the adoption of a cloud solution, the rationale should support a specific business need.

For each option, the business case should include an analysis of the cost model with identified costs, benefits, pricing model, contractual adjustments, variation to contracts, and any changes in budgetary appropriation types. The level of detail provided for each option should be commensurate with its level of investment and risk.

3.5 Prepare an exit strategy

An exit strategy is critical for a cloud solution as it documents the agency's contingency plan to migrate records securely to another solution, non-cloud or cloud, while maintaining business continuity. For data stored by the CSP, the agency must also consider what data will need to be archived, where it will be archived, the method to transfer it, how it will be destroyed and how destruction will be verified together with the security requirements associated with these processes. Liabilities should be clearly defined in the contractual terms and cover breaches beyond the life of the contract. Agencies should review key requirements for data backup, bulk transfer and format standards as mentioned below under *Functionality* and *Standards*. *Records Management in the Cloud* also provides further guidance. The costs associated with the exit strategy should be accounted for in the cost model and the business case.

The exit strategy must also consider the likely business scenarios that may be required. Scenarios could include the inability of the CSP to meet performance requirements, CSP security breaches or issues involving CSP business viability.

3.6 Determine contractual terms

Prior to approaching the market agencies should determine the contractual terms they will require, even when they anticipate a standardised 'click wrap' agreement to be the only option. A prior understanding of the agency's terms will provide a basis to ensure the final contract will meet business requirements, security requirements and adequately address the risks associated with the cloud solution.

Agencies should refer to *Negotiating the cloud – legal issues in cloud computing agreements* as a starting point for defining contractual terms. The guide details the contractual mechanisms to manage risks.

3.7 Approach the market

Agencies should determine the most appropriate model — for example, cloud computing, managed services, outsourcing, in-house delivery or hybrids of these — for the business problem being addressed.

Agencies must meet the usual requirements that apply to procurement, including compliance with Commonwealth Procurement Rules (CPRs) and agency Chief Executive Instructions. Agencies must also comply with whole-of-government ICT coordinated procurement arrangements.

When drafting procurement documentation, agencies should consider the following areas:

- clearly define the business problem;
- outline the agency's needs and constraints clearly — for example, what is the scope, the rationale behind moving to a cloud solution or indeed whether you go to the market for all types of solutions including a cloud solution; and
- are there any constraints surrounding legislation, regulation, legacy systems, integration, connectivity, availability, information security and integrity, etc.

Agencies may choose to use the Data Centre as a Service (DCaaS) multi-use list (MUL) which will be available for use by agencies in November 2012. The aim of the MUL is to provide the smaller 50 percent of agencies with a means to identify potential suppliers of cloud and cloud-like services. The MUL may also be used by larger agencies, state and territory governments and other Commonwealth bodies.

The MUL will provide agencies with a common approach to sourcing solutions for contracts which are less than $80,000 and less than 12 months. To be included on the DCaaS MUL suppliers will have signed a deed giving agencies confidence that they are dealing with reputable suppliers. The DCaaS initiative will also incorporate post-delivery assessments (feedback) by agencies to help identify *bona fide* providers from those that have proven to lack the appropriate capabilities.

3.8 Select a provider

Like any procurement, selecting a CSP involves verifying that the business needs and security requirements are fully addressed in the contractual arrangements and that the outcome is based on the value for money principle.

Agencies should validate the cost model against the CSP's pricing considering the following:

- assure pricing is transparent, e.g. subscription or pay-as-you-go pricing, upgrades, maintenance and exit costs;
- costs for unexpected peaks in demand;
- require service price for upgrade and maintenance fees appropriate to the services being procured, some upgrades may be automatic and included in the service;
- confirm the cost model is suitable and allows for scaling and changes to service;
- look for commitment requirements, such as minimum use;
- confirm setup, training and integration fees; and
- request references to clarify ongoing cost of service.

In addition to the considerations in *Cloud Computing Security Considerations*, agencies should consider the following as they evaluate requirements:

- look for requirements which may not fit into the CSP's existing pre-configured templates and may increase the cost of configuration;
- confirm the CSP's ability to meet service levels, noting the CSPs will likely have differing service level definitions and capabilities;
- confirm the ability to monitor CSP service levels;
- confirm the CSP's architecture will meet scalability, availability, capacity and performance guarantees and is sufficient for agency requirements;

- confirm any multi-tenancy arrangements and their impact on security requirements;
- determine any foreign laws which may impact the CSP and the data it stores;
- confirm where the CSP's data will be located, including any transborder data transfer, if applicable;
- confirm the CSP's willingness to allow audits, particularly in multi-tenancy arrangements; and
- confirm the CSP's disaster recovery (DR) capability meets the agency's requirements;
  - if necessary, ask for proof that the supplier conducts DR exercises which confirm the ability to fail key production components to a secondary data centre with documented disaster recovery procedures, and
  - key elements of proof include the ability to access to network, components and applications while maintaining data currency, and evidence of processes to keep DR plans, scripts and procedures reviewed and updated;

3.9 Plan for implementation and on-going operations

The planning required in a cloud solution implementation is similar to that of an outsourcing arrangement. Agencies will require an internal project to manage those activities which will need to be done in-house. Such activities typically include:

- preparatory work to make application and infrastructure ready for integration with the cloud solution;
- perform risk and security assessments;
- updating business continuity plans;
- preparing an end of life plan to disengage with the provider and transition service and data while assuring business continuity;
- updating architectural artefacts;
- performing acceptance testing; and
- managing business transition and organisational change.

Agencies must also put in place the internal capability and resources need to manage the cloud service on a daily basis. Ongoing operational activities include:

- monitoring performance and service levels;
- responding to incidents and service disruptions;
- analysing, coordinating, prioritising and implementing configuration changes to meet emerging requirements and user feedback;
- managing configuration documentation;
- coordinating planned upgrades or outages;
- reconciling invoices against services provided;
- managing the relationship with the CSP;
- administering governance arrangements; and
- handling service or contract disputes.

Agencies will need to clearly define processes, procedures, roles and responsibilities for these activities, clearly specifying which tasks must be done in-house and which will be done by the CSP.

Where changes to internal skills are required, agencies must ensure the necessary organisational changes are in place so sufficient in-house resources are in place to meet the requirements for on-going operations.

4. Review the implementation

Agencies should conduct a post-implementation review after the implementation to:

- undertake periodic risk assessments for information held in the cloud;
- compare the value and benefits of cloud solution against the business case;
- capture lessons learned from the implementation, operation and support of the cloud service;
- prioritise any new business changes; and
- provide feedback through AGIMO and the CLIC to other government agencies.

Attachment 1 – Cloud business management checklist

Agencies should use this checklist in conjunction with the recommendations provided in the guide. The left column indicates the related section. By acknowledging the completion of items in this checklist, the user confirms the consideration of all advice provided in the guide.

Establish strategic direction which begins with low risk applications or pilots and draws on lessons learned for future endeavours to capitalise on potential benefits of cloud-based services

2	**Engage with the AGIMO** and the Cloud Information Community to identify opportunities	□
2.1	**Assess suitable business needs** to determine which information types and business processes will benefit the most from cloud-based services and their related technical impacts	□
2.2	**Consider triggers and timing**, identifying upcoming initiatives which present opportunities for the use of cloud-based services	□
2.3	**Consider financial impacts**, including whole of life costs and changes to capital/operational expenditure, and ensure they are reflected in the agency's capital management plan, income statement and balance sheet	□
2.4	**Consider organisational capability**, considering the strategic impact to the organisation structure and skills sets and have a plan to mature capabilities in targeted areas	□
2.5	**Manage change**, obtaining senior executive sponsorship and engaging stakeholders to address resistance and ensure successful take-up of cloud-based services	□
2.6	**Review governance** to ensure controls are adequate for cloud computing	□

Implement a cloud solution as a structured project

3.1	**Build a business model** to provide business context, estimate lifecycle cost and to form the basis for functional, performance and resource requirements	□
3.2	**Assess the risks** and determine suitable treatment strategies	□
3.3	**Capture requirements** for functionality, standards, performance, manageability, security and compliance	□
3.4	**Build a business case**, providing business rationale and an assessment of options	□
3.5	**Prepare an exit strategy** which considers business continuity, disposition of data and exit costs	□
3.6	**Determine contractual terms** prior to engaging the market	□

3.7	**Approach the market**, ensuring compliance with CPRs and agency CEIs	□
3.8	**Select a provider**, verifying claims on costs, architecture, reputation and capability	□
3.9	**Plan the implementation**, ensuring sufficient resources to prepare infrastructure and manage organisational change	□
3.9	**Prepare for on-going operations**, ensuring sufficient in-house resources will be in place for on-going operations	□

Review the implementation

4	**Undertake periodic risk assessments** for information held in the cloud	□
4	**Confirm the benefits** to ensure cloud solution provides the value and benefits expected in the business case	□
4	**Capture lessons learned** and apply to future cloud-based services	□
4	**Prioritise any new business changes**	□
4	**Provide feedback to AGIMO** and the CLIC	□

Attachment 2 – Business case template for a cloud solution

The business case should discuss the options available to solve a business problem. The option to deploy a cloud solution should be weighed against available alternatives, such as in-house COTS solutions, rather than advocating a single, preferred solution. For each option, the business case should include the likely costs, potential savings, procurement and contractual arrangements and an overview of the perceived risks, which may contribute to the weakness of the option.

The following section of the guide steps through the structure of a business case which presumes that a proposed cloud solution is preferred, having been objectively assessed to provide more value for money with adequate security over other alternatives. Agencies should use the business and cost models to make such an assessment.

The completed business case will be subject to the agency's investment decision-making process and should be reviewed by the agency's architectural design authority or similar body.

1. Executive summary

1.1 Summary of Options

Use the executive summary to provide a brief description of the current situation and the proposed response through deployment of a cloud computing solution. Provide a summary of the available options including initial cost estimates, proposed savings and the strengths and weaknesses of each option. Consider using a table format similar to the one below:

Option One: *Option name* **Brief Description:** *Include a one line description of the option* **Vendor:** *Name of the proposed cloud computing vendor* **Total Cost:** *$XX million* **Total Savings:** *$XX million* **Option Lifespan:** *N years*		
Strengths	**Weaknesses**	**Recommendation**
Option Two: *Option name* **Brief Description:** *Include a one line description of the option* **Vendor:** *Name of the proposed cloud computing vendor* **Total Cost:** *$XX million* **Total Savings:** *$XX million* **Option Lifespan:** *N years*		

Strengths	Weaknesses	Recommendation

1.2 Financial Summary

Include a financial summary of the options in a table format similar to the one below:

		Year 1	Year 2	Year 3	Year 4	Total
		$'000 (NPV)	**$'000 (NPV)**	**$'000 (NPV)**	**$'000 (NPV)**	**$'000 (NPV)**
Option One	Capital*					
	Operational**					
	Total					
Option Two	Capital*					
	Operational**					
	Total					
Option Three	Capital*					
	Operational**					
	Total					
Option Four	Capital*					
	Operational**					
	Total					

*Capital: Note the expected reduction in ICT capital expenditure arising from the adoption of cloud computing solution. Show any reductions in capital expenditure using a negative sign, e.g. -$1,000.

** Operational expenditure includes transfers of capital expenditure funding to operating expenditure.

Note: Use net present value (NPV) with an appropriate discounting factor for financial estimates.

2 Current Situation

This section sets out the issue/opportunity that proposal seeks to address. Provide an overview of the current situation, setting the context for the agency, business, stakeholder situation, technical environment and current risks.

2.1 Policy/Agency Context

State the business objective that would be realised through the available solutions. Compare the objective with the agency's strategic priorities. Refer directly to the outcomes and outputs in your agency's Portfolio Budget Statements, corporate plan and annual report. Include the identification of any relevant agency risks that contribute to the triggering situation for the proposal.

2.2 Current Technical Environment

As a business case for a cloud solution is ICT enabled, describe the current situation not only from a business perspective – but also from a current technical perspective. This section documents the relevant components of your current ICT baseline. For example, the section should briefly describe:

- ICT infrastructure (both hardware and software)
- Extent of virtualisation across the agency
- Voice and data communications facilities
- Workforce skills and numbers
- Security

The section must describe any gaps that the project must address to meet the Critical Success Factors and performance indicators. Gaps may be specific elements or more general service levels related to current levels of interoperability, security and efficiency.

The purpose of this step is to clarify your ICT environment as it stands and any shortfalls. It is not useful to revisit past developments and events at this point. High level environment and architecture diagrams can be helpful, but keep in mind the audience for the document when thinking about the degree of technical detail to include.

2.3 Business Problem

Your cloud business case should begin by stating the practical business problem that options for deploying a cloud computing solution could help to overcome in achieving the government's policy and service delivery objectives.

Deployment of a cloud computing solution may address several business problems, including:

- Facilitating virtualisation across the agency (introductory, intermediate and advanced levels of virtualisation)
- Providing a low cost option for systems development work through cloud computing options (rather than investing in ICT infrastructure for new development work)
- Enhancing the level of service delivered to stakeholders through rapid elasticity and flexibility of service provision utilising a cloud computing vendor
- Reducing agency and whole-of-government costs, such as:
  - reduced ICT costs through higher utilisation of infrastructure (optimisation)
  - re-use of existing assets
  - volume discounts
  - standardisation and simplification
- Speed to implement
- Overcoming the limitation and constraints of a current solution

2.4 Stakeholder Impact

Describe the impact of the current situation on stakeholders.

2.5 Current Risks

Describe the risks that the current situation creates, and the risks of not responding to the current situation. Include both business and technical risks.

2.5 Current Costs

The ability to determine total cost of ownership (TCO) of existing systems will depend on the extent and maturity of the agency's ICT cost management practices. Data may be available from the CIO or CFO group on:

- annual ICT BAU budgets for specific systems;
- charge-back costs to the business unit for specific systems or ICT business support;
- specific supplier expense costs such as hosting or consulting; and
- previous project costs to compare development alternatives.

Where TCO or whole-of-life costs cannot be adequately determined due to a lack of data, a cost comparison of known costs may be sufficient to compare solutions. This involves a break-down of known or reasonably estimated costs for the legacy system and the Cloud solution alternative (eg licensing, development, customisation, hosting, maintenance etc). The business case should always attempt to compare like-for-like costs, and clearly identify where this is not the case, and where any assumptions have been made.

3 Proposed Response

Having identified why the business case is being developed, the proposed response section outlines what is being proposed to be done in response. This is about identifying the desired end state or destination, rather than the detail how to get there.

Include a description of the proposed response with any evidence that this will be an effective response to the current situation. This section should focus on 'what' is being proposed as a response, rather than 'how' that response can be delivered.

3.1 Strategic Alignment

Identify how the adoption of a cloud solution aligns with your agency objectives listed in the policy/agency context section. Refer to your agency's Portfolio Budget Statements to identify the outcomes that delivery of this response would support.

- Where relevant provide specific reference to your agency's ICT strategic vision and, where appropriate, AGIMO's *Cloud Computing Strategic Direction paper*.

The technical environment and business environment sections that follow should describe the vision of the future state of the organisation, i.e. what will be different about the current situation from both a technical and business perspective as a result of the proposed response.

3.2 Technical Environment

Describe the future state of the technical environment based on the proposed response (not the specific options). High level environment and architecture diagrams can be helpful, but keep in mind the audience for the document when thinking about the degree of technical detail to include.

3.3 Business Environment

Describe the future state of the business operational environment based on the proposed response.

3.4 Benefits

Provide a statement of the benefits that the project will achieve and indicative timing for when they will be realised. Include information on how benefits will be measured and the expected targets to be achieved for each measure.

Include interim and longer term benefits, and include any identified negative implications (which might be fluctuations in user-pay provisions of the contract, penalties for breaches of service level standards by the CSP, etc).

4 Proposal Summary

A summary of the information provided about the current situation, the proposed intervention using cloud solution options and the expected benefits.

A high level visual representation of the cloud solution might be helpful.

5 Solution Options

5.1 Design Criteria

Include where possible the high level requirements that any viable cloud computing solution will be expected to deliver against. Note the high-level business requirements that the solution must address. Consider areas such as:

- changes in business practices;
- transitional considerations;
- security considerations;
- dependencies across ICT platforms and architecture;
- reliability, availability and maintainability;
- usability, flexibility, scalability, interoperability;
- speed to deploy; and
- major external interfaces.

These requirements provide the criteria for comparing options. Indications of relative value across the options will be informative.

5.2 Identified Options

The business case must consider the available options from a range of differing cloud computing approaches to using in-house or non-cloud capabilities. The agency's capacity to adapt business processes and support the introduction of changes in culture will also be important considerations in the evaluation of options.

The outcome will be a shortlist of options for analysis and comparison in the initial cost-benefit analysis. Normally this shortlist will include a base case (maintaining existing arrangements), a "do minimum" case (to address only urgent and unavoidable requirements) and two to three other options.

Provide the detail of each option in the Option Details section.

6 Options Analysis

Summarise the most significant features of each option. Present a tabular comparison of the options against costs, savings, contract flexibility, implementation timeframe, design requirements listed above and risk. Note any preferences in a "Conclusions" line.

The table below presents a possible presentation.

Requirement	Option 1	Option 2	Option 3	Option N
Benefits				
Disadvantages				
Total costs				
Total savings				
Flexibility of the contract				
Estimated implementation timeframe				
Requirement 1				
Requirement 2				
Requirement N				
Implementation risks				
Conclusion				

7 Implementation Approach

Having identified the problem to be solved and the options to be explored in response, this section of the business case is about confirming the agency's capability and capacity to deliver the preferred cloud solution.

Describe the implementation approach for delivering the cloud solution, including the approach to market, the project/program management governance structures and other key control and assurance processes, describing variations for each identified option if different.

Make note of any changes that will occur in the organisation's culture that will support the deployment of the cloud solution

It may also be appropriate to provide a visual representation of the implementation through a roadmap, illustrating how the vision, implementation strategy and delivery strategy interrelate leading to the adoption of the solution.

8 Agency Capability

The purpose of this section of the business case is to provide agency decision makers and stakeholders with sufficient context to inform any decision it might make based on the agency's organisational capability.

Identify targeted capability areas in project management, procurement/contract management, relationship management and service management which will have to be addressed. Identify required skill sets and determine which will need to be procured or developed in-house. Propose a high-level approach to mature capability in targeted areas. Include any costs in the business case.

The government has adopted the Portfolio, Programme and Project Management Maturity Model (P3M3®) as the common methodology for assessing organisational capability. The model can help agencies identify capability areas which will need to be addressed.

9 Security and information assurance

This section is intended to discuss the issues associated with security and information assurance in respect of the proposed cloud solution.

In terms of security, the business case should identify whether there are increased issues in relation to security arising from the move to a cloud solution rather than a non-cloud ICT solution. In particular, addressing the following areas in terms of security will be important:

- The security classification/dissemination limiting marker and type of information being processed and stored.
- A summary of the security issues that relate to the proposed cloud solution.
- A risk-based assessment of the information to be stored in the cloud.
- An overview of the agency's security assessment mechanisms that are used to determine whether CSPs have appropriate standards in place to meet the security requirements of customers.
    - A CSP may have its own security standards frameworks, which can be summarised for this part of the business case, e.g. the CSP may use cloud encryption gateways to provide cloud security proxies or utilise specific quality assurance protocols for data transactions concerning individuals or businesses.
- A description of the type of security services offered by the preferred CSP, e.g. firewalls, intrusion detection systems, intrusion prevention systems, antivirus services, distributed denial-of-service protection services, messaging security and web gateway security services.

For information assurance, the business case should cover the following issues:

- Agency standards for information assurance and expectations that a cloud vendor will align with the standards as agreed in contractual arrangements.
- The steps that the agency will take to ensure that the agreed information assurance standards are adhered to by the vendor during the life of the contract.
- Any agency specific business processes that are used as part of an information assurance model that are to be replicated by the cloud computing vendor.
- An evaluation of information assurance for the CSP's services in comparison to the agency's enterprise services.

- Focus on whether the cloud vendor offers high-assurance services that meet the agency's requirements and whether a higher premium is paid by the client for high levels of assurance.

10 Risks

A high level risk analysis should be undertaken to identify the key risks and the potential mitigating actions associated with cloud computing options. Risks should be ranked according to the agency's established risk management procedures. Refer to the DoFR *Better Practice Guide on Risk Management*[11] for more detailed guidance.

The following table provides some examples of risks and mitigating responses:

Key strategic risk	Risk rating*	Mitigating action
Business practices are not well understood prior to seeking cloud-based services via a vendor.		Agency to conduct business processing mapping and analysis to identify business processes that will be efficiently managed through cloud computing solutions.
Commercial arrangements for cloud-based services are not well understood by the agency.		Agency to seek advice from their procurement area on the nature of commercial arrangements associated with contracts with cloud vendors.
Business services with medium/high level risks are potentially identified for a cloud solution.		Agencies to undertake scoping work to identify business services carrying low risk and potentially the most feasible services to transition to a cloud solution.
Business continuity failure as a result of vendor with low capability.		Agency to determine capability of CSPs during the commercial assessment of the tender evaluation.
Security & information assurance failures.		Agency to determine the physical location of data storage under a cloud arrangement and to seek security/information assurance guarantees from cloud vendor. Only those services carrying low security risks should be in scope of provision via a cloud computing vendor.

* Risks are rated according to the agency's established risk management procedures.

11 Summary of option details

Repeat this section of the business case for each option, including the following subsections:

- Description
- Stakeholder Impact
- Costs
- Savings
- Benefit
- Summary Cost Benefit Analysis
- Risk
- Timeframe

[11] http://www.finance.gov.au/comcover/better-practice-guide.html

12 Critical success factors

An analysis of Critical Success Factors (CSFs) can be useful in determining how well each option compares against the project investment options and benefits criteria. CSFs are defined as:

> *"The attributes that are used to determine the successful delivery of the programme and which the available options are assessed against."*

CSFs will naturally vary from project to project and it is suggested that agencies consider the CSFs for each project on a case by case basis and involve key stakeholders in determining the CSFs.

An example of a CSF high level analysis is shown below.

Key CSFs	Description
CSF1: Business needs	An identification of how the option meets agreed investment objectives, related business needs and service requirements.
CSF2: Strategic fit	A description of how well the option aligns with the agency's ICT strategic plan and key elements of their forward work plan.
CSF3: Value for Money	Identification of the option's value for money.
CSF4: Achievability	A description of whether the option is considered to be achievable from the perspective of the agency's change management/adoption capabilities, whether the agency possesses the requisite skills to implement the option and whether key stakeholders support the option.
CSF5: Supply side (vendor) capability and capacity to deliver services	A key element in any cloud computing proposal is an assessment of the cloud computing vendor capability and capacity to deliver contracted services. Part of this assessment should also consider the competitiveness of the specific segment(s) of the cloud market (e.g. IaaS, SaaS and PaaS) and whether market offerings are likely to provide a cost-effective solution to the agency.