Australian Government
Information Management Office

# Community Cloud Governance – An Australian Government perspective

Better Practice Guide

## Contents

## Introduction

A Community Cloud is one of four cloud models outlined in the *Australian Government Cloud Computing Strategic Direction Paper*[1] (the Strategy), released in April 2011. The other models are public cloud, private cloud and hybrid cloud. The Strategy defines a Community Cloud as "cloud computing services shared by several organisations that have shared requirements, e.g. mission, security requirements, policy, and compliance considerations". A Community Cloud may support those agencies with a common delivery agenda to take advantage of the benefits that may be realised by cloud computing services (also known as cloud services).

Cloud services are those services delivered via "an *ICT sourcing and delivery* model for enabling 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". The Strategy states that agencies may choose to use cloud services if it provides value for money and adequate security.

The Australian Government is looking to the benefits of cloud services as a way of reducing redundancy and duplication across agencies, and seeking to realise economic savings and improved business outcomes.

Appropriate governance arrangements must be in place before agencies may transition any type of ICT arrangement. Community Clouds are no exception. Appropriate governance

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

arrangements should provide agencies with the structure to establish; deliver; and consume cloud services as well as oversee their performance and alignment with strategic goals and policies.

This guide has been developed in accordance with the principles outlined by the Australian National Audit Office (ANAO) in their *Public Sector Governance Better Practice Guide*[2] (2003) and the Cross Agency Governance Principles outlined in the Australian Government's *ICT Customisation and Bespoke Development Policy* (EM 2009/57). It also takes into account ICT governance industry standards, namely *AS 8015-2005 Corporate Governance of Information and Communication Technology* and *ISO/IEC 38500:2008 Corporate Governance of Information Technology*.

This guide aims to provide agencies with guidance on implementing *Community Cloud Governance* from an Australian Government perspective based on related *frameworks* using formal *agreements* that are managed by well defined *governance structures* with clear *roles and responsibilities.*

### Applicability

This guide is applicable to:

- Australian Government agencies establishing a Community Cloud that uses private or public sector cloud services. Cloud services may be provided by ICT systems that support the operations and assets of agencies, including ICT systems provided or managed by other agencies, third party service providers, or other sources.
- All cloud service models, e.g. infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), as defined by the Strategy.

### Terminology

For terminology associated with community cloud computing, refer to Attachment 5: Terminology in the Strategy. This guide extends the definition of "Community Cloud" to encompass the concept of a "Government Cloud" provided, for example, by a Lead Agency.

In many Community Cloud arrangements, Lead Agencies are also Participating Agencies. References to Lead Agencies in this guide refer to the Lead Agency's role outside of being a participant of the community cloud.

A list of Acronyms can be found at Attachment 3.

## Governance

Good governance ensures that the business of government is being conducted properly. Governance provides the structure, guidance and controls for operating a Community Cloud, ensuring the effective and equitable use of agency resources.

Whether a Community Cloud is newly established or been operating for a number of years, the Governance Model should clearly outline the roles and responsibilities of participants, an agreed funding model; and an agreed process for dispute resolution. It should also outline how agencies would join and leave the Community Cloud.

The Lead Agency is responsible for establishing and managing a Governance Committee and a Governance framework that will manage the operation of the Community Cloud.

[2] http://www.anao.gov.au/Publications/Better-Practice-Guides/2005-2006/Public-Sector-Governance

In establishing a Community Cloud, Lead Agencies should:

- Through contractual arrangements, ensure that the Community Cloud Service Provider (CCSP) takes a principles-based approach to cloud service delivery. The Lead Agency should also address the Australian Government's requirements to security and privacy ensuring that the CCSP complies with any legislative and regulatory requirements.
- Establish a written and agreed Community Cloud Agreement (CCA), noting that:
  - Terms and conditions of participation will need to be agreed by agencies. To suit business requirements, agencies may participate in more than one Community Cloud;
  - A Community Cloud should enable Participating Agencies to be mobile, for example, machinery of government (MOG) changes may require movement from one Community Cloud to another with minimum difficulty; and
  - There may be two Lead Agency roles where the role of the CCSP is undertaken by an agency.

In some instances, there may be an existing formal arrangement in place between agencies, for example, a memorandum of understanding (MoU). In these cases, the MoU should be examined for its suitability for the management of Community Cloud and modified as required.

The following sections provide guidance on the content that Lead Agencies should include in its contractual arrangements with a CCSP and in drafting a CCA.

## Governance principles and standards

Agencies, having varying sizes, complexities, structures and legislative backgrounds, operate within a complex environment. It is important therefore, that in establishing a Community Cloud governance framework the elements of good governance be applied.

In developing the framework, it is recommended that agencies refer to following documents:

- The ANAO's Better Practice Guide: *Public Sector Governance and the Individual Officer*[2], published in 2003, states that "Governance, in a public sector scenario, is the set of responsibilities and practices, policies and procedures, that provide strategic direction, manage risks and use resources responsibly and with accountability to ensure objectives are achieved". This document sets out principles for public sector governance:
  1. **Accountability** — being answerable for decisions and having meaningful mechanisms in place to ensure adherence to applicable standards;
  2. **Transparency** — clear roles and responsibilities and clear procedures for decision making and the exercise of power;
  3. **Integrity** — acting impartially, ethically and in the interests of the agency, and not misusing information acquired through a position of trust;
  4. **Stewardship** — using every opportunity to enhance the value of the public assets and institutions that have been entrusted to care;
  5. **Efficiency** — the best use of resources to further the aims of the organisations with a commitment to evidence-based strategies for improvement;
  6. **Leadership —** leadership from the top is critical to achieving an agency-wide commitment to good governance.

- The Australian Public Service Commission's 2007 publication, *Building Better Governance*, outlined the common features that make up a well-constructed governance framework:
  - Strong leadership, culture and communication
  - Appropriate governance committee structures
  - Clear accountability mechanisms

  - Working effectively across organisational boundaries
  - Comprehensive risk management, compliance and assurance systems
  - Strategic planning, performance monitoring and evaluation
  - Flexible and evolving principles-based systems.

- The Australian Government's *ICT Customisation and Bespoke Development Policy* (EM 2009/57) which sets out guiding principles for cross agency governance. It is recommended that Principles 1 and 2 below be applied in the governance arrangements for a Community Cloud Agreement.
  1. The Lead Agency must have a written Cross Agency Agreement in place with Participating Agencies.
  2. Agencies should have a Governance Committee and a Governance Model in place to manage the ongoing use, development and support of the software solution(s). Agencies involved in Cross-Agency arrangements will collaborate with the intent to reduce customisation and bespoke development wherever possible.
- *Audit Report No 41, Performance Audit on Effective Cross-Agency Agreements*[3], 2009-10. This report examined a cross-section of agreements to determine if they were generally fit-for-purpose and consistent with sound essential information to inform better practice.
- *AS 8015-2005 – Corporate Governance of Information and Communication Technology*[4] – this standard provides guiding principles for directors of organisations on the effective, efficient and acceptable use of ICT within their organisation. It applies to the governance of resources, computer-based or otherwise, used to provide information and communication services to an organisation. *ISO/IEC 38500:2008 Corporate Governance of information technology*[5] is the equivalent international standard (based on AS 8015-2005).
- *Information Privacy Principles*[6] and the *National Privacy Principles*[7], found within the Privacy Act 1988. These principles are managed by the Office of the Australian Information Commissioner (OAIC).
- *OAIC Information Principles*[8], found on the Australian Government's Office of the Australian Information Commissioner (OAIC) website.
- *Digital Continuity Principles*[9], found on the National Archives of Australia (NAA) website.

## Community Cloud Agreements

In establishing a Community Cloud, there should be a written and agreed document, the CCA, which sets out the parties together with the terms and conditions for participation. The parties would include the Lead Agencies and the Participating Agencies. It may include the CCSP where the CCSP is an agency (in some instances, the CCSP may have the role of Lead Agency). This agreement will need to be agreed by all parties prior to commencement of the cloud services.

In drafting a CCA, agencies should consider using the Collaborative Head Agreement Template within the *National Collaboration Framework*[10] (NCF). This framework was established to assist

[3] http://www.anao.gov.au/uploads/documents/2009-10_Audit_Report_41.pdf

[4] http://www.ramin.com.au/itgovernance/as8015.html

[5] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51639

[6] http://www.privacy.gov.au/materials/types/infosheets/view/6541

[7] http://www.privacy.gov.au/materials/types/infosheets/view/6583

[8] http://www.oaic.gov.au/publications/agency_resources/principles_on_psi_short.pdf

[9] http://www.naa.gov.au/records-management/agency/digital/digital-continuity/principles/

Australian Government agencies, state/territory and local jurisdictions to work collaboratively together.

In those cases where the Lead Agency is an Australian Government agency, the Lead Agency will need to comply with the Commonwealth Procurement Rules (CPRs) and other areas in drafting a CCA. The following section covers other governance areas which must be considered.

## Other Governance Considerations

When establishing governance for a Community Cloud service, agencies need to include the following considerations.

### *Security*

Security must be integrated into any governance framework for the adoption of cloud computing by Australian Government Agencies. When using the cloud, agencies need to be able to set controls that govern the security of their information, including access control and user verification.

Australian Government agencies participating in a Community Cloud, either as a provider or consumer of cloud services, should take a risk-based approach in accordance with Australian Standard for Risk Management AS/NZS ISO 31000:2009; and Australian Standards HB 167:2006 Security risk management.

Agencies should refer to the Defence Signals Directorate (DSD) *Cloud Computing Security Considerations*[11] which provides a list of controls around the security and risk considerations for cloud computing, including potential issues with data sovereignty and aggregated data, when undertaking any risk assessment.

Australian Government agencies participating in a Community Cloud must comply with the requirements of the:

- *Protective Security Policy Framework (PSPF)*[12] which sets out the Australian Government policy and guidance on protective security; and
- *Information Security Manual (ISM)*[13], the standard that governs the security of government ICT systems, and which complements the PSPF.

### *Security Classifications*

Agencies seeking to join a Community Cloud should verify that the security classification of the Community Cloud are equivalent (or higher) to the security classification of the agency's information and ICT networks. For example, if a Community Cloud operates at a security classification of PROTECTED, then the agency can only receive, through the cloud, information classified up to the security classification supported by their ICT network. Information classified as PROTECTED or UNCLASSIFIED may be stored in this Community Cloud, but information classified at a higher level must not be stored in it. Agencies should refer to the PSPF and ISM for further information.

[10] http://www.finance.gov.au/e-government/better-practice-and-collaboration/national-collaboration-framework.html

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

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

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

Agencies should be aware of and take into consideration the full protective security capabilities of the CCSP, its staff, facilities, procedures and technologies. Participating Agencies including the Lead Agency must ensure that their risk assessment addresses these issues.

### Standards

Conceptually, interoperability is best achieved through the use of industry recognised open standards. While cloud computing is not a new technology, existing standards need to be amended and new standards implemented where necessary. Given the global nature of cloud computing, this work involves a balancing act between global and national interests in issues surrounding interoperability, data portability, and security. Having international standards in place will provide a level of assurance for agencies that these issues have been considered. It should be pointed out that even compliance with standards will not provide the complete solution. It will be necessary for Lead and Participating Agencies in each Community Cloud to assess and determine the necessary characteristics that will meet their interoperability, data portability, and security requirements and undertake the architectural design and implementation accordingly.

However, until the international standards development work has been completed, resolution of these issues will be best achieved, in the short to medium term, through Community Clouds ensuring that the appropriate levels of security, interoperability, and data portability are factored into any architectural design work.

### Compliance

Agencies and CCSPs will need to comply with legislative and regulatory requirements.

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

- Department of Finance and Deregulation circulars and advice including whole of government ICT policies, strategies, frameworks and policies, for example, use of the Internet-based Network Connections Service panel for wide area network and internet connections, and the Internet Gateway Reduction program for Internet gateways.
- Business continuity management requirements given that the business aspects required under a business continuity plan will shape the delivery requirements of a cloud service.
- Agency-specific procurement policies.
- Agency-specific security policies.

The Australian Government Cloud Computing Better Practice Guides have been developed to provide both agencies and CCSPs with guidance on transitioning to the cloud. The Better Practice Guides include:

1. *Cloud Computing Security Considerations*
2. *Privacy and Cloud Computing for Australian Government Agencies*
3. *Negotiating the Cloud – Legal Issues in Cloud Computing Agreements*
4. *Financial Considerations for Government in Cloud Computing*
5. *Records Management and the Cloud*[14].

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

## Community Cloud Governance Structure – an example

An example Community Cloud Governance Structure has been provided to enable agencies to understand the roles and responsibilities within a community Cloud environment.

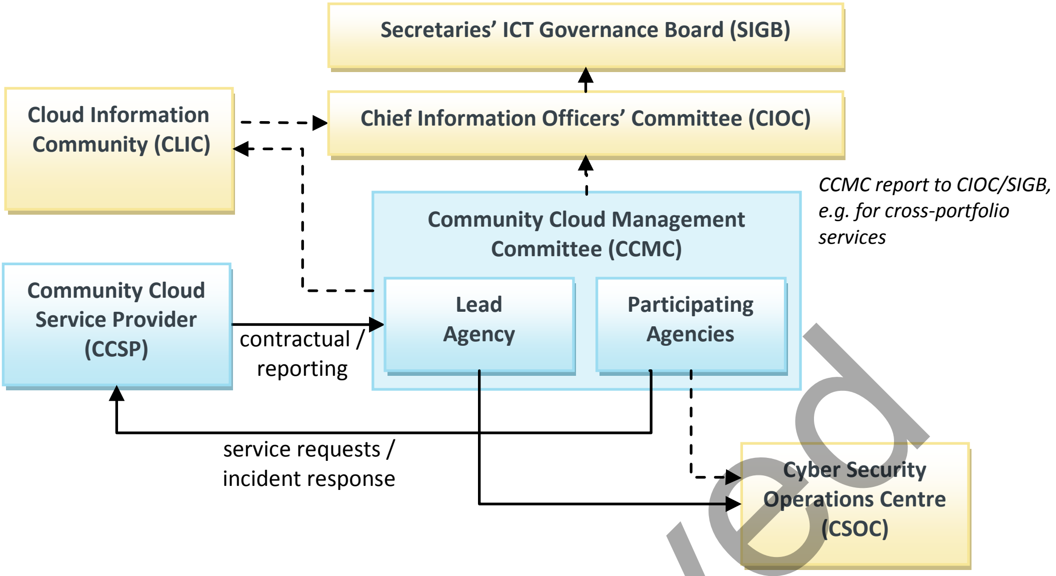
Secretaries' ICT Governance Board (SIGB)
Chief Information Officers' Committee (CIOC)
Cloud Information Community (CLIC)
CCMC report to CIOC/SIGB, e.g. for cross-portfolio services
Community Cloud Management Committee (CCMC)
Community Cloud Service Provider (CCSP)
contractual / reporting
Lead Agency
Participating Agencies
service requests / incident response
Cyber Security Operations Centre (CSOC)

**Figure 1. Example Community Cloud Governance Structure**

Figure 1 represents an example of governance arrangements for a Community Cloud and associated reporting lines.

The participants in this scenario include:

1. **Community Cloud Management Committee** (CCMC) — this Committee would be established to set policy and make decisions for a particular Community Cloud, oversee activities, and progress and issues escalated by the agency participants.
2. **Lead Agency** — the Lead Agency would be responsible for providing a leadership role in a Community Cloud, managing relationships with Participating Agencies, managing and reporting on the contractual relationship with the CCSP, and providing an escalation point for any issues between Participating Agencies and the CCSP.
3. **Participating Agencies** — Participating Agencies are those agencies that receive Community Cloud services provided by the CCSP and generally interact directly with the CCSP for service management, issue resolution and reporting.
4. **Community Cloud Service Providers** (CCSP) — the CCSP provides Community Cloud services. A CCSP can be either a commercial third party or an agency. Where CCSP services are provided by an agency, the agency may also share the Lead Agency role.
5. **Cloud Information Community** (CLIC) — the CLIC provides a forum for sharing information on areas of common interest across agencies, and to facilitate the free flow of information. The role of the CLIC in this scenario is as information gathering. Community Cloud participants would be members of the CLIC.
6. **CIOC** — CIOC may be a participant in some Community Cloud governance arrangements, in particular where services cross more than one portfolio.
7. **SIGB** — SIGB may be a participant in some Community Cloud governance arrangements, in particular where services cross more than one portfolio.

**Attachment 1: Governance Roles and Responsibilities** provides examples of the responsibilities and activities for each participant in the governance arrangement.

**Attachment 2: Governance Checklist** provides a checklist that identifies the governance issues discussed in this guide.

# Attachment 1: Governance Roles and Responsibilities

## Community Cloud Management Committee

A CCMC should be established to set policy and make decisions for each Community Cloud. This may be an existing committee or a new committee. The role of this committee is to oversee the activities, progress and issues of the agency participants and to provide a contact point with the CCSP (under the arrangements agreed by the Lead Agency). The CCMC may choose to meet with or without the involvement of the CCSP.

Membership of the CCMC should include one representative from the Lead Agency plus one from each Participating Agency.

A sample list of CCMC responsibilities are:

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Policy | Undertake role of Policy Management Authority (PMA). | Policy decisions<br>Consensus decision-making |
| Governance performance | Provide overall governance for the Community Cloud.<br>Liaise with Lead and Participating representatives to resolve issues, concerns and progress of the Community Cloud. | Funding oversight and management<br>Oversight of development, establishment and ongoing support for the Community Cloud<br>Establish common development paths consistent with the agreed strategy to improve the overall efficiency, effectiveness, and interoperability of the cloud services offered by the Community Cloud. |
| Security requirements | Endorse policy for security standards and requirements within the Community Cloud. | Security requirements and standards |
| Integrity and Trust | Oversee that there is an ongoing high level of integrity and trust within the Community Cloud. | Trusted environment |
| Communication | Provide a forum to share information on issues, concerns and progress of the CCSP. | Effective communication and consultation |

## Lead Agency

The Lead Agency for a Community Cloud should manage the CCMC. The Lead Agency is responsible for providing a leadership role in a Community Cloud; managing relationships with Participating Agencies; and managing the contractual relationship with the CCSP. Lead Agencies would undertake the role of Chair of the CCMC, provide secretariat services to the CCMC, and participate in the CLIC.

A sample list of Lead Agency responsibilities are:

### *Administration*

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Reporting | • Provide reports and advice to SIGB as required on the progress and position of the Community Cloud operations, developments and issues.<br>• Provide reports and advice to the CCMC on the status and position of the Community Cloud operations, development and issues<br>• Under contractual arrangements, receive reports and advice from the CCSP on the operation and management of the Community Cloud as required. | Reports and Advice |
| Governance Committees | • Provide chair to CCMC.<br>• Provide a representative member to CCMC.<br>• Provide CCMC secretariat services. The Secretariat should be the point of contact between the Lead and Participating Agencies.<br>• Provide a representative member to the CLIC. | CCMC membership<br>CCMC meeting administration, reporting and management<br>CLIC membership |
| Information Exchange | • Distribute CCMC information and documentation amongst committee members, through the secretariat.<br>• Communicate community cloud progress, experiences, concerns and issues for discussion. | Community Cloud information exchange |

### *Establishment / Implementation*

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Business Requirements | • Gather and manage initial set of business and service requirements of Participating Agencies.<br>• Prioritise initial set of business and service requirements through governance processes. | Business Requirements<br>Service Requirements Management processes |
| Security Requirements | • Gather and manage mandatory security requirements as set out in the PSPF and the ISM.<br>• Prioritise non-mandatory (desirable) security requirements through governance processes.<br>• Ensure any potential CCSP can meet mandatory security requirements prior to selection. | Security Requirements |
| Procurement | • Organise, evaluate and manage approaches to market (ATMs)[15], including drafting release to market, and receipt of their | Procurement management including RFT documentation |

[15] ATMs include Requests for Tender (RFTs), Requests for Information (RFIs), Requests for Quote (RFQs), Expressions of Interest (EOIs), etc.

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| | responses, through the Contract Management function. Evaluate tenders and manage CCSP selections and contractual arrangements on behalf of the Community Cloud.<br>• Transition to contract<br>• Manage procurement of CCSPs on behalf of the Participating Agencies. Activities include:<br>  • Collection of business and service requirements from Participating Agencies (including service levels)<br>  • Creation, management, review and release of ATMs<br>  • Receipt of information responses and tenders from CCSPs<br>  • Coordination and evaluation of tenders<br>  • Management of CCSP selections and contractual arrangements. | and reporting<br>Negotiation report<br>Contract |
| Contract management | • Organise, manage and review service level agreements and contractual arrangements, using requirements obtained from Participating Agencies. Includes service levels for common or individual agency agreements. | Contract management<br>Management of Service Level Agreements (SLAs) |
| Relationship management | • Create, manage and review CCA between parties to the CCA.<br>• Manage Lead Agency/Participating Agency relationships with the community cloud: adding, amending, withdrawing and supporting participants.<br>• Assist Participating Agencies as they transition, participate in, and exit the Community Cloud. | CCA with each Participating Agency<br>Participating Agency Relationship Management processes |
| Strategic Direction | • Work with Participating Agencies to ensure that the operational and strategic alignment continues to deliver the benefits of a Community Cloud to Participating Agencies. | Strategy implemented |
| Service Catalogue Management | • Oversee development of Service Catalogue and processes.<br>• Negotiate content of Service Catalogues on behalf of Participating Agencies.<br>• Forward Service Catalogues from CCSPs to Participating Agencies.<br>• Prioritise enhancements and changes to the Service Catalogue.<br>• Coordinate decisions on requests for change from Participating Agencies (jointly with impacted CCSP). Communicate decisions to Participating Agencies requesting change.<br>• Forward endorsed changes to impacted CCSPs.<br>• While the CCSP could have a range of cloud services that it can put into a Community Cloud, Lead and Participating Agencies should agree a baseline set of cloud services that they require. Negotiating the cost of the agreed cloud services will be through the governance arrangements. | Service Catalogue Management processes<br>Service Catalogues distribution<br>Management of change requests |

### *Operational*

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Governance | • Lead Agency to provide Community Cloud services and ensure that CCSP is operating in accordance with SLAs.<br>• Manage relationships and issues arising between Participating Agencies and CCSPs. | Issues Management processes<br>Issues exchange and resolution |
| Contract management | • Manage contractual relationship with CCSP<br>• Organise, manage and review CCSP contracts and SLAs.<br>• Add, amend, withdraw and support a CCSP as appropriate. | Contract management |
| Compliance | • Manage / monitor compliance with legislation, regulations, certifications, accreditations and standards.<br>• Ensure that the operation and management of the Community Cloud is consistent with Australian Government regulations and directions on issues regarding commercial agreements, and financial responsibility and delegations.<br>• Ensure that the operation and management of the Community Cloud should be consistent with Australian Government whole of government policies, strategies and frameworks including principles, regulations and directions on issues concerning, but not limited to, cloud computing, security, identity and access management, information management. | Compliance Management / Monitoring processes |
| Financial Management | • Manage billing arrangements with each CCSP. Includes cost variations and increases from CPI / other reasons.<br>• Manage billing arrangements with participating agencies (if applicable). | Financial / billing management processes |
| Relationship Management | • Manage Participating Agency relationships within the community: adding, amending, withdrawing, supporting. | Participating Agency relationship management processes |
| Security Management | • Manage and maintain the state of security and incident response and reporting to the Cyber Security Operations Centre (CSOC). | Security Management processes in place |
| Service Catalogues | • Manage changes to Service Catalogues. Manage decisions and endorsement on change requests. | Service Catalogue management processes |
| Issues Management | • Manage and resolve issues between the CCSP and Participating Agencies.<br>• Manage and resolve issues including faults and incidents with the CCSP. | Issues resolution |
| Risk Management | • Manage risks identified with the Cloud Community. | Risk management processes |
| Change Management | • Coordinate Change Management control of releases and updates from CCSPs and Participating Agencies. | Change approved and implemented |
| Support Services | • Manage complaints from Participating Agencies and their resolutions. | Complaints managed |
| Information Exchange | • Provide Community Cloud information management governance, e.g.<br>  • Sharing information with Participating Agencies<br>  • Updates (periodic / regular) to Services Catalogue | Information management processes |

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
|  | • Information security, privacy and user access. |  |

## Participating Agencies

Participating Agencies are those agencies that participate in the Community Cloud, that is, they are provided with cloud services. They may or may not have direct contact with the CCSP.

A sample list of Participating Agency responsibilities are:

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Committee membership | • Provide a representative member to CCMC or user group.<br>• Provide a representative member to CLIC (optional).<br>• Note: full representation may be impractical for Communities where membership is greater than 10. | CCMC membership [larger communities could develop a User Group type of consultative committee]<br>CLIC membership |
| Contract Management | • Negotiate, where applicable, and agree to a CCA. | CCA |
| Service Requirements | • Forward service requirements for service provision to the Lead Agency. These requirements should contribute to the negotiations between the Lead Agency and the CCSPs on the content of their Services Catalogues. Any changes to a Services Catalogue that have been instigated by a Participating Agency should be communicated to the Lead Agency for coordination of a decision, endorsement and passage to the impacted CCSP. | Service Requirements |
| Performance Management | • Monitor and review:<br>  • Activity performance and service levels achieved against contractual agreements with CCSPs.<br>  • The agency's activity performance against the CCA. | Monitor performance<br>Activity Reports |
| Issues Management | • Communicate any issues with CCSP activities and expectations, including faults and incidents, through the Contract Management function of the Lead Agency. This should be undertaken in a timely manner. | Communicate issues to CCSPs |
| Service Catalogue Management | • Inform the Lead Agency of requirement to update the CCSP Services Catalogue .<br>• Forward request for enhancements to the Lead Agency. | Service Catalogue Change Requests |
| Security Management | • Incident response and reporting (to Lead Agency or CSOC). | Security incident management |
| Information Management | • Manage the ongoing ownership of Participating Agency information. | Information management |
| Support services | • Manage complaints from customers and users with an escalation process established in line with contractual arrangements. | Complaints management |

## Community Cloud Service Provider (CCSP)

An agency (either the Lead Agency or another agency) or a commercial third party may operate as the CCSP and provide cloud services on behalf of the Community Cloud. Where an agency is the CCSP, the Lead Agency role and responsibilities may be shared.

A sample list of CCSP responsibilities are:

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| CCSP Service Delivery | • Under contractual arrangements or SLAs, provide appropriately secure Community Cloud services together with the applications, systems and supporting infrastructure that will satisfy the requirements of the Community Cloud Participating Agencies.<br>• Deliver efficient and cost effective Community Cloud services. | Compliant community cloud services, applications, systems, security and supporting infrastructure<br>Supporting CCSP personnel |
| Financial model | • Under contractual arrangements or SLAs, provide unit-based pricing for elastically (up/down) scalable on demand cloud services. | Transparent pricing |
| Compliance | • Under contractual arrangements or SLAs, comply with legislation, regulations, certifications, accreditations and standards.<br>• Operation and management of the Community Cloud should be consistent with Australian Government policies, strategies and frameworks including principles, regulations and directions on issues concerning, but not limited to, cloud computing, security, identity and access management, information management, and carriage services.<br>• Implement security requirements and report any breaches. | Compliance management / Monitoring processes |
| Reporting | • Provide reports and advice to the Lead Agency and the CCMC as required under contractual arrangements or SLAs, on the progress and position of the Community Cloud operations, developments and issues. | Reports and Advice |
| Service Catalogue Management | • Provide a 'Services Catalogue' that clearly defines the cloud services that will be available in the Community Cloud and the cost of cloud services to each agency.<br>• Update the Service Catalogue on a regular (agreed interval) basis as more cloud services become available, or in response to endorsed changes requested by the CCMC.<br>• Forward to the Lead Agency:<br>  • A initial draft set of cloud services for negotiation by the Cloud Community<br>  • A finalised and agreed Service Catalogue of cloud services<br>  • Updates to the Service Catalogue resulting from regular cloud services updates/reviews and endorsed changes requested by Participating Agencies. | Service Offerings<br>Service Catalogues<br>Service Updates |
| Issue Management | • Address and resolve issues, including faults and incidents that are raised by Lead and Participating Agencies and brought to its attention, within an agreed period of time.<br>• Communicate issues for the attention of Participating Agencies through the Contract Management function of the Lead Agency. | Issues exchange and resolution |
| Information Management | • Provide stewardship of Participating Agencies' information in line with contractual arrangements. | Information managed |
| Support | • Provide agreed Help Desk / Service Support for the Community | Help Desk / Service Support |

| | | |
|---|---|---|
| Management | Cloud and its participants to agreed SLAs. | processes |

## Cloud Information Community (CLIC)

The CLIC was established in 2010 to provide agencies with a forum to share information on areas of common interest across agencies, and to facilitate the free flow of information. It is coordinated by AGIMO. Membership of the CLIC should include Lead Agency representatives and Participating Agencies as necessary. The Terms of Reference for the CLIC can be found on the CLIC Govdex website[16].

A sample list of CLIC responsibilities are:

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Information Exchange | - Facilitate community cloud information exchange amongst members. | Community Cloud Information Exchange, including: Community Cloud computing issues; and advice on technologies. |

## CIO Committee (CIOC)

Reporting to SIGB, the CIOC addresses the priorities determined by the Ministers Committee on ICT, providing 'thought leadership' in the ICT arena, identifying strategic issues, and is a forum for exchange of information between agencies.

The CIOC investigates, identifies and endorses ICT issues and emerging trends that can be applied at a whole of government level. Issue-specific working groups support it. The CIOC makes recommendations to SIBG regarding whole of government service delivery strategy and business impact. It provides expert technical advice to SIGB.

The Australian Government Chief Information Officer chairs the CIOC and membership comprises representatives of central bodies, portfolio departments and delivery agencies.

A sample list of CIOC responsibilities are:

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Strategy | - Provide strategic direction to Lead Agencies on Community Cloud activities.<br>- Channel directions from SIGB to Lead Agencies on Community Cloud issues | Strategic Direction |
| Reporting | - Receive reports and advice from CCMC on cloud services, trends, concerns and issues (as required) | Reporting and Advice |

[16] https://www.govdex.gov.au/confluence/display/CLIC/

### Secretaries ICT Governance Board (SIGB)

SIGB is responsible for the development of WofG strategies; determining priority areas for standardisation, consolidation and common approaches to ICT usage across the Australian Government. It also determines the Australian Government's response to emerging ICT trends and issues such as cloud computing. The Terms of Reference for SIGB can be found at http://www.finance.gov.au/e-government/strategy-and-governance/ict-governance-committees.html.

A sample list of SIGB responsibilities are:

| Activity | Responsibilities | Deliverables / Outcomes |
|---|---|---|
| Strategy | • Provide strategic direction to Lead Agencies on Community Cloud activities. | Strategic Direction |
| Reporting | • Receive reports and advice from CCMC on cloud services, trends, concerns and issues (as required) | Reporting and Advice |

## Attachment 2: Governance Checklist

The following checklist identifies the governance issues discussed in the guide. In contemplating a community cloud governance framework, an organisation should ensure that these issues are addressed.

A particular community cloud may raise additional governance issues. Agencies should always ensure that they have undertaken a thorough review of, and obtained necessary specific advice on, any governance arrangement they are considering participating within.

| | |
|---|---|
| **Community Cloud Agreement (CCA)**<br>When creating the CCA, your agency must consider the following:<br>• Has the CCA been agreed to and been signed by all parties?<br>• Does the CCA have mechanisms for varying the agreement?<br>• Does the CCA comply with the National Collaboration Framework (NCF)? | □ |
| When establishing the **Community Cloud Management Committee** and **Governance Model** to manage the ongoing development and support for the CCA, your agency must consider the following:<br>**Community Cloud Management Committee (CCMC)**<br>• Have you, where possible, used an existing committee and existing structure to avoid duplication?<br>• Does the CCMC have representation from a representative selection of Participating Agencies to the CCA?<br>• Does the CCMC have an agreed Terms of Reference?<br>• Do the Terms of Reference align with the Better Practice principles outlined in ANAO's Effective Cross-Agency Agreements, Audit Report No. 41 and the Cross-Agency Governance Principles?<br>**Community Cloud Governance Model**<br>• Does the Community Cloud Governance Model list the roles and responsibilities of parties to the Community Cloud Agreement?<br>• Does the Community Cloud Governance Model contain an agreed funding model?<br>• Does the Community Cloud Governance Model have an agreed process for issue and risk management, enhancement requests and dispute resolution?<br>• Does your Governance Model align with the Better Practice principles outlined in ANAO's *Effective Cross-Agency Agreements, Audit Report No. 41*? | □ |
| **Community Cloud**<br>When establishing a Community Cloud, the following should be considered:<br>• Have you agreed the baseline set of cloud services for the Community Cloud?<br>• Have you considered the impact of Cloud Computing to your IT networks and business | □ |

| | |
|---|---|
| processes?<br>• Have you considered the future intentions for the use of the cloud solution?<br>• Have you considered any impact of Cloud Computing on service delivery?<br>• Is there a genuine business need for the establishment of a Community Cloud?<br>• Does the Community Cloud align with legislative and regulatory requirements as well as WofG policies, strategies and frameworks? | |

## Attachment 3: Acronyms

| | |
|---|---|
| AGIMO | Australian Government Information Management Office |
| ANAO | Australian National Audit Office |
| AS | Australian Standard |
| ATM | Approach to Market |
| CCA | Community Cloud Agreement |
| CCMC | Community Cloud Management Committee |
| CCSP | Community Cloud Service Provider |
| CIOC | Chief Information Officers' Committee |
| CLIC | Cloud Information Community |
| CPI | Consumer Price Index |
| CPR | Commonwealth Procurement Rules |
| CSOC | Cyber Security Operations Centre |
| EM | Executive Memorandum |
| IaaS | Infrastructure as a Service |
| ICT | Information and Communication Technology |
| IEC | International Electrotechnical Commission |
| ISM | Australian Government Information Security Manual |
| ISO | International Organization for Standardization |
| MOG | Machinery of Government |
| MoU | Memorandum of Understanding |
| NAA | National Archives of Australia |
| NCF | National Collaboration Framework |
| OAIC | Office of the Australian Information Commissioner |
| PaaS | Platform as a Service |
| PMA | Policy Management Authority |
| PSPF | Protective Security Policy Framework |
| SaaS | Software as a Service |
| SIGB | Secretaries' ICT Governance Board |
| SLA | Service Level Agreement |