PART F – STATEMENT OF REQUIREMENT

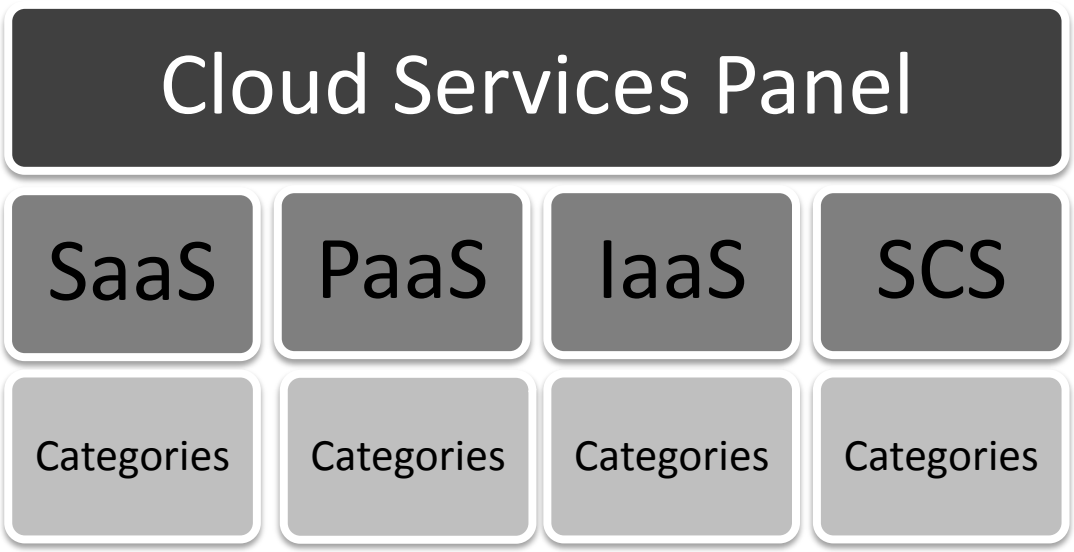
Whole-of-Government Cloud Services Panel Structure

The Whole-of-Government Cloud Services Panel (**Cloud Services Panel**) comprises four Service Models, which include Software as a Service (**SaaS**), Platform as a Service (**PaaS**), Infrastructure as a Service (**IaaS**) and Specialist Cloud Services (**SCS**). The Service Models, with the exception of the SCS, are defined as per the National Institute of Standards and Technology (**NIST**) definitions (see definition of Cloud Computing). SCS[1] is defined as:

"Consultancy support services associated with the different Service Models. These may include services to transfer data/configuration between service providers, management and support of applications (workloads) operating on Cloud Services Panel services, multi supplier service integration services and cloud strategy and implementation services."

The following diagram illustrates the current structure of the Cloud Services Panel.

Figure 1: Current Structure of the Cloud Services Panel



Finance is proposing to remove the nine Categories limit from the existing Panel structure, allowing Panellists to add services to the appropriate Service Model.

Finance will continue to seek to add new suppliers to the Cloud Services Panel every 12 to 18 months through an open approach to market. Finance reserves the right to add or remove Cloud Services or Categories of Cloud Services from the Service Catalogue at its discretion.

Tenderers are capped at submission of three Cloud Services for evaluation only. Should a Tenderer's submission be successful for any Service Model, they will be able to propose more Cloud Services in any Service Model for inclusion in the Service Catalogue. Finance will consider these proposals after it has refreshed the Panel and using the process in the Head Agreement for establishing the Service Catalogue.

[1] http://govstore.service.gov.uk/cloudstore/

Scope of Service

In Scope

The Cloud Services that are within scope of the Panel must demonstrate the Essential Characteristics of Cloud Services as defined by NIST:

- **On-demand Self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- **Broad Network Access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- **Resource Pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.
- **Rapid Elasticity**: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured Service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

SaaS, PaaS, or IaaS Cloud Services are considered in scope if they meet the:

a. above Essential Characteristics of Cloud Computing;

b. Service Model specific requirements for SaaS, PaaS or IaaS (as applicable) described in the Service Model Response Template; and

SCS services are considered in scope if they meet the Service Model specific requirements for SCS as described in the Service Model Response Template.

Out of Scope

Cloud Services that are out of scope of the Panel are:

- services that do not meet the definition of Cloud as defined by NIST;
- services that do not meet Service Model and Category specific requirements; and
- any services or products provided under existing whole of government coordinated procurement initiatives listed on Finance's website.

Reporting

Successful Tenderers will be required to report to Finance any business they conduct through the Cloud Services Panel via the ICT Procurement Portal. As noted in the Head Agreement, reporting requirements may include details of Contracts entered into between Successful Tenderers and Agencies, such as: Agency name and contact details; Tracking Number, Contract financial value; Term; Commencement Date; end date; description and quantity of Cloud Services provided; Service Model; Service Category; vendor SKU; and purchase order details. Reporting requirements could also include actual Agency Cloud Services consumption information over time. This information may include spend by Agency by month, invoice numbers, invoice dates and Cloud Services consumed. Successful Tenderers are required to provide copies of all invoices and Schedule 3: Contracts to Finance.

As a preference, Finance will use the ICT Procurement Portal to collect reporting data from Successful Tenderers. However, Finance may elect to use other electronic means such as a common spreadsheet format. Finance will communicate final formats and templates to Successful Tenderers prior to the Panel's commencement. Finance may change the reporting requirements and means of collecting reporting data as the Panel matures.

Tenderers are required to submit evidence of their reporting capabilities, such as a sample report with similar data fields to those mentioned above, as part of their Tender. Tenderers should demonstrate an ability to generate Agency contract reporting and Agency invoice or consumption reporting.

Account Management

Tenderers are required to submit a statement to support their account management capabilities, including an appropriate escalation structure for raising issues. Tenderers should demonstrate suitable internal structures and procedures to adequately support Finance and Customers in regard to the Cloud Services supplied under the Head Agreement and Contracts.

Service Catalogue, Quoting, Contracting and Invoicing

Finance has implemented an electronic Service Catalogue of Successful Tenderers' Cloud Services under the Panel. The Service Catalogue allows Agencies to browse Cloud Services available through the Panel and request quotations from Panellists. Successful Tenderers will be expected to utilise the electronic systems via secure portals and will be able to respond to quote requests and report on executed contracts and invoices. Finance will, where possible, use the data recorded through electronic systems to generate reporting data.

Where it is not practicable for Finance to implement electronic systems, more conventional methods for quoting, contracting, invoicing and reporting will prevail.

Standards and Industry Accreditation

Where a Tenderer has described compliance with an internationally or industry recognised standard or accreditation, Finance requires formal evidence of the Tenderer meeting the standard or holding current accreditation. This may be in the form of a certificate of currency from the standard or accreditation body, which clearly identifies the validity of the Tenderer's claims, or similar authenticable evidence.

Tenderers are required to provide this evidence as attachments to their Tender. Tenderers should strictly limit attachments to documentation that identifies the current nature of the standard or accreditation.

Security Classifications, Certification and Assessment

Agencies have varying security requirements for storing data. When procuring Cloud Services, Agencies will require adequate security certifications, audits and clearances that are commensurate with the nature and sensitivity of data stored in the Cloud.

The Attorney-General's Department is responsible for the Australian Government security classification system and the application of protective markings. Tenderers should consider offering Cloud Services that meet varying Agency security requirements.

Where Agencies seek to store data (other than publically available data) in the Cloud, for each Cloud Service where applicable, Tenderers may be required to undertake the following:

a. gateway certification by the Australian Signals Directorate (ASD);

b. IT security audit by a certified Information Security Registered Assessors Program (IRAP) assessor;

c. security vetting of Tenderer's staff in accordance with the Australian Government Security Vetting Agency (AGSVA);

d. ASIO-T4 protective security audit of the Tenderer's data centre by the Australian Security Intelligence Organisation (ASIO);

e. continuing compliance with 'Strategies to Mitigate Targeted Cyber Intrusions' by ASD; and

f. any other relevant jurisdictional requirements or standards.

Where a Tenderer claims to have successfully completed any of the above certifications, Finance requires evidence to be attached in the Tender to support its claim. Tenderers should strictly limit attachments to documentation that identifies the current nature of the certification or accreditation.

Location of the Data Centre

Where a Tenderer claims that its data centre is located within Australian Territories to provide a Cloud Service, the Tenderer must submit evidence to support its claim.

If the Tenderer leases data centre facilities from a third party within Australian Territories, the Tenderer should provide supporting evidence of the lease agreement and premises location. Supporting evidence could include individual pages from a lease agreement, which identify the address of the leased facilities, and the lease agreement signature page.

Tenderers should strictly limit attachments to documentation that identifies the location of the data centre where required. Finance does not require evidence of data centres outside Australian Territories, unless specifically requested by Finance.

Attachments and supplemental information

Where a Tenderer elects to, or is required to include attachments, supplemental information or evidence, it should strictly limit attachments to relevant documentation. Finance reserves the right not to consider this information if it deems the information irrelevant to the Tender.

Specifications

SCS

All Cloud Services offered by a Tenderer in the SCS Service Model are required to satisfy the Service Model specific requirements in the the Service Model Response Template.

SCS is the provision of specialist consultancy services that have direct focus or relation to cloud computing and services. Areas of specialty may include, but are not limited to:

a. Cloud on-boarding, deployment and transition management;

b. Cloud integration and optimisation;

c. design and development of Cloud applications (e.g. online forms, surveys, SharePoint sites);

d. data conversion, cleansing and migration onto Cloud; and/or

e. Cloud project specification and selection.

IaaS, PaaS and SaaS

All Cloud Services offered by a Tenderer that fall under the IaaS, PaaS and SaaS Service Models are required to satisfy the minimum content requirements. The specific requirements for each Service Model are included in the statement of requirements provided with the Service Model Response Template.

The requirements for each of these Service Models are as follows:

a. On-demand Self-service;

b. Broad Network Access;

c. Resource Pooling;

d. Rapid Elasticity; and

e. Measured Service.

Completing the response template

The RFT includes a commercial and compliance response template (consisting of Parts E1 to E6) for Tenderer to include its details, reporting capabilities, its commercial capabilities and compliance with the Head Agreement. The RFT also includes a technical and pricing

response template that Tenderers are required to complete to tender a Cloud Service. Each Service Model Response Template contains five parts:

a. **the Cloud specific requirement questions** – for each Cloud Service a Tenderer should answer these questions for the Cloud Service to be considered under the Cloud Services Panel;

b. **Service Model Specific requirements** - each Cloud Service tendered by must these requirements to be considered a Cloud Service which falls within that specific Service Model;

c. **Cloud Service Specific Conditions and Service level Information** - Finance requires Tenderers to provide details on the Cloud Service they are tendering and has allowed Tenderers to provide a detailed description of their Cloud Service (capped at 100 words). Tenderers also need to complete the specific conditions and service level information for each of the Cloud Services;

d. **Service Model specific pricing scenario** - a pricing scenario that requires the Tenderer to quote for the Cloud Service for which Finance has provided the required specifications. The template allows Tenderers to provide any assumptions or qualifications that will impact on the final pricing;

e. **Cloud Service specific referee details** - Finance requires Tenderers to provide details of a referee for every Cloud Service they are tendering for. It is highly desirable that the Tenderer's dealings with the provided referee have occurred within the last 12 months; and the

Tenderers should ensure that, when completing the columns for each of the offerings, they include the information requested for each Cloud Service description and the cost for that Service. The cost variables for each Cloud Service must be specified.

Panel requirement vs. Agency requirement

Finance has aimed to be intentionally high level in the requests for information for this RFT process. Agencies will have the opportunity to issue Requests for Quotes (RFQ) under this Panel in which they will be able to seek responses for Agency specific requirements from Panellists. The specification table contains high level information on the Cloud Services and offerings that the Panellist can provide and is not intended to be constraining. Panellists will be able to bundle Cloud Services in response to RFQs, provided that all the Cloud Services they bundle are listed on the Service Catalogue.