Buying Cloud Services in Public Sector

Handbook - Including Sample RFP Language for a Cloud Framework Agreement

Version 2: February 2022

Notices

This document is provided for informational purposes only. It has not been developed in accordance with legal requirements for public procurement processes within any particular region. Cloud customers are responsible for making their own independent assessment of the information in this document and any use of a cloud provider's products or services. This document does not create any warranties, representations, contractual commitments, conditions or assurances.

Sample documents and language should not be construed as legal advice, guidance or counsel. Cloud customers should consult their own legal advisors about their responsibilities under the applicable law in their own country of operations. CISPE expressly disclaims any warranties or responsibility or damages associated with or arising out of information provided within this document.

About CISPE

CISPE (*Cloud Infrastructure Services Providers in Europe*, https://cispe.cloud) is non-profit independent industry group. We represent cloud infrastructure service providers in Europe, working with industry and policymakers to provide guidance and education on Cloud services and their role in industry, public life and society in general.

Our growing membership includes companies operating in all EU countries and globally headquartered 16 European countries. The association is open to companies provided they declare that at least one of their services meets the requirements of the CISPE Data Protection Code of Conduct. We:

- Advocate the benefits of cloud first public procurement policies within EU and EU Member States
- Engage the Cloud infrastructure sector to reach Climate Neutrality by 2030
- Promote coherent EU-wide security requirements and technical standards
- Support comprehensive privacy requirements with a Data Protection Code of Conduct
- Work to keep the EU cloud infrastructure market open, competitive and free from lock-in
- Prevent unjustified content monitoring obligations in the EU legal framework

Our members deliver and maintain the essential "building blocks for IT" that make it possible for government, public authorities and businesses to build their own systems and deliver essential services to billions of citizens. In this role, we are helping to enable the development of leading-edge technologies and services incorporating Artificial Intelligence (AI), Connected Objects, autonomous vehicles and 5G, and the next generation of cellular connectivity technology.

Code of Conduct for Cloud Infrastructure Services

The CISPE Data Protection Code of Conduct, publicly launched in September 2016, pre-dated enforcement of the European Union General Data Protection Regulation (GDPR). It aligns with strict GDPR requirements to help cloud infrastructure providers to operationalize data protection compliance and offer a strong framework to help customers select cloud providers and trust their services. The CISPE Code of Conduct has been validated by the European Data Protection Board (EDPB) in May 2021, and approved by the French CNIL acting as the Competent Authority in June 2021. https://www.codeofconduct.cloud/

Climate Neutral Data Centre Pact

CISPE engaged with the European Commission at the end of 2019 to develop a set of metrics and a self-regulatory initiative to ensure climate neutrality of data centres by 2030. This initiative has been developed together with the European Data Centre Association (EUDCA) along with other trade associations and data centres market players - launched in January 2021 as the "Climate Neutral Data Centre Pact" https://www.climateneutraldatacentre.net/

Fair Software Initiative

Together with the French CIO association CIGREF, and with the support of other trade associations of CIOs and Providers across Europe, CISPE has launched 10 Principles of Fair Software Licensing for Cloud Customers, a set of best practice for business looking to the cloud for growth innovation and flexibility, and challenge their software providers to ensure fair licensing terms are referenced.
https://www.fairsoftware.cloud/

GAIA-X

CISPE was one of the twenty-two founding members of GAIA-X – the European initiative to deliver an open, transparent and secure digital ecosystem. As such CISPE has been committed to the vision and principles of the GAIA-X organisation from the outset and its Secretary General has been re-elected in June 2021 to serve on the board of directors. Some of the tools referenced in the handbook such as the CISPE Data Protection Code of Conduct, and the SWIPO IaaS Code of Conduct are useful to demonstrate compliance with the GAIA-X principles. https://www.gaia-x.eu

CISPE and the Public Sector

CISPE contributes to the European public policy debate and works to ensure a better understanding of the role, contribution and potential of Europe's cloud infrastructure industry.

While public purchase models should condition the process of adopting and using cloud computing, acquiring cloud services differs from most traditional technology acquisitions known to the public sector. Procurement approaches need to be rethought: CISPE is encouraging EU policymakers to develop a more ambitious and forward-looking approach at EU scale based on "cloud first" policy initiatives, helping to drive the growth of the single cloud infrastructure market in Europe and underpinning Digital Single Market (DSM) growth goals.

This handbook is designed to provide helpful guidance and support to public authorities when procuring cloud services.

More information

CISPE members: https://cispe.cloud/members
Executive Board: https://cispe.cloud/board-of-directors
Cloud computing services declared under CISPE Code of Conduct:
https://www.codeofconduct.cloud/public-register/

Table of Contents

Summary and purpose of this Handbook

The purpose of this **Buying Cloud Services Handbook** is to provide guidance to those Cloud customers wishing to purchase Cloud Services through a competitive procurement process (**Cloud Services Request for Proposal- RFP**), but lacking the expertise to draft a Cloud Framework Agreement.

This document is provided for informational purposes only. It has not been developed in accordance with legal requirements for public procurement processes within any particular country or region.

The handbook also looks as additional selection criteria language for **Call Offs** or **Mini Competitions** when purchasing off of a Cloud Framework Agreement. The sections of the handbook are organized to resemble a generic IT RFP. Sample generic RFP and selection criteria language is accompanied by commentary to help understand why a cloud RFP is different from a traditional IT RFP.

Following the publication of the EU Commission Cloud Strategy guiding how the European Institutions and Agencies will modernize their IT Infrastructure through a cloud-first approach, CISPE handed over the handbook to the EU Commission in July 2019 during the event '*How to transform governments through a smart cloud policy*'.

Version 2 of this handbook includes new guidance regarding; data protection (section 2.3.1.1), switching cloud providers and porting data (section 2.3.1.2), software terms and conditions (section 2.5.2), sustainability in the cloud (section 3.6), and a refreshed Appendix B Live Technical Evaluation.

> ***'Cloud Services'*** *refers to all of the cloud technologies and related services that an end user may need access to. It includes consulting or professional/managed services need to support and execute migration to the cloud and support workloads on the cloud, in addition to cloud infrastructure itself, and cloud marketplace services such as Software as a Service (SaaS) products.*

The emergence of cloud computing as the default choice for public sector IT presents an opportunity to modernize existing procurement strategies. Cloud-centric acquisition processes can enable public sector entities to extract the full benefits of the cloud, such as access to leading-edge innovation, increased speed and agility, improved security posture and compliance governance—whilst realizing efficiencies and cost savings.

Traditional IT procurement methods for buying hardware, software and data centres do not translate to buying cloud services. Approaches to pricing, contract governance, terms & conditions, security, technical

requirements, SLAs and more all change in a cloud model, and using existing procurement methods ultimately reduces or eliminates the benefits that cloud provides.

One of the best means of effective public sector acquisition of cloud services is with a **Cloud Framework Agreement** – a multi-organizational award of a menu of clouds, from which eligible purchasers affiliated with the purchasing organization can acquire the cloud technologies and associated services that meet and suit their needs. As a vehicle for cloud contracts, such framework agreements enable purchasing of cloud services in an efficient and effective manner—resulting in purchasing organizations and end user entities having access to a full range of cloud services, and ultimately reaping the full benefits of the cloud: agility, benefit from massive economies of scale, scalability to reach a better availability at lower cost, breadth of functionality, pace of innovation, capacity to scale to new geographies.

Note that **this paper focuses on the purchase of Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud technologies, as provided by a *Cloud Infrastructure Service Provider (CISP)*.** Such cloud technologies can be purchased directly from a CISP, or through a CISP Reseller. *Additional RFP considerations would be required for distributors of cloud marketplace services (PaaS and SaaS), and cloud consulting services.*

Also note that this paper does not cover every aspect of creating an end-to-end cloud procurement framework. There are many other documents from industry and analysts covering issues such as cloud procurement best practices, how to budget for cloud, cloud governance, etc., and we strongly recommend that such advice and papers are taken into account while developing an overall cloud procurement strategy. **Table 1** below provides an outline of the Cloud Services RFP Handbook, and where sample RFP language is located for each component of a cloud services RFP.

Table 1 – Summary of Cloud Services RFP Handbook Sections

Section	Overview and Sample RFP Language
0 Overview of a Cloud Framework Agreement	A high-level view of the cloud framework agreement model (LOTs, how to compete, and contracting)
2.0 Cloud Services RFP Overview	Sample generic RFP language covering the below sections, along with commentary explaining the rationale behind the Cloud Services RFP structure and language used.
2.1 Cloud Services RFP Setup	2.1.1 Introduction and Strategic Objectives 2.1.2 RFP Response Timeline 2.1.3 Definitions 2.1.4 Detailed Description of the Buying Model and Competing within the Framework Agreement 2.1.5 Bidder Minimum Requirements - Administrative
2.2 Technical	2.2.1 Minimum Requirements 2.2.2 Comparison between Vendors 2.2.3 Contracting
2.3 Security	2.3.1 Minimum Requirements 2.3.1.1 Data Protection 2.3.1.2. Switching Cloud Providers and Porting Data 2.3.2. Comparison Between Vendors 2.3.3 Contracting
2.4 Pricing	2.4.1 Minimum Requirements

Section	Overview and Sample RFP Language
	2.4.2 Comparison between Vendors
2.5 Contract Execution Setup/T&Cs	2.5.1 Terms and Conditions 2.5.2 Software Terms and Conditions 2.5.3 How to Select Between Awardees 2.5.4. On-Boarding and Off-boarding
3.0 Best Practices/Lessons Learned	3.1 Cloud Governance 3.2 Budgeting for Cloud 3.3 Understand Partner Business Model 3.4 Cloud Brokers 3.5 Pre-RFP Sourcing/market research 3.6 Sustainability
Appendix A – Technical Requirements for Comparison between Bidders	A list of generic cloud technology requirements for Call Offs or Mini Competitions
Appendix B – Live Technical Evaluation	A sample script for cloud technology product demonstrating scoring (cloud demos as part of a Call Off or Mini Competition)

1.0 Overview of a Cloud Framework Agreement

A well-designed cloud framework agreement can enable the purchasing of cloud services in a way that benefits both the participating public sector organizations and cloud vendors. Benefits of a well-designed cloud framework agreement include:

- Cooperative in Nature:
    - Multiple organizations banding together to place orders for similar requirements means convenience, efficiency, reduced costs, as well as a simplified ordering process. It establishes an effective way to aggregate multiple public sector organizations' demand for common cloud technologies and associated cloud services such as marketplace solutions and consulting.
- Full Range of Cloud Services:
    - It can include in-scope all of the consulting/professional/managed services needed to fully support and execute the migration to the cloud and supporting workloads on the cloud, in addition to CISP-provided cloud technologies, and marketplace services.
    - Cloud technologies can be purchased directly from a CISP or through a designated reseller.
- Contract Governance:
    - It aligns disparate organizations/purchasers around a common set of terms and conditions and a single master contract award, rather than different ones for each organization.
    - It is also of benefit to vendors as it provides a standard acquisition process, terms and conditions, and ordering mechanism to navigate rather than different ones for each public sector organization.
    - It provides flexibility. Creating, approving and running an effective cloud contract within existing government policies/regulations requires experimentation and the ability to adjust quickly. It is much more beneficial to create a framework agreement that allows the public sector and cloud vendors to all work together to improve the contract – contractually, mechanically, and efficiently. A multi-year contract that does not work and cannot be adjusted leads to a poor experience for public sector end-users, procurement organizations and cloud vendors
- Choice:
    - It enables purchasers to choose between several qualified CISPs, and sets a high-bar for all cloud services and associated services such as a cloud PaaS/SaaS marketplace, and cloud consulting.
    - It allows for control over the number of suppliers on a framework through ensuring that the standard of each awardee is appropriately vetted.

A framework agreement to buy cloud services works best when it includes core CISP-provided IaaS/PaaS technologies, along with a PaaS/SaaS marketplace, and the consulting services that public sector end-users can access, when needed, to help them plan, transition, utilize and maintain a workload running in the

cloud. We therefore suggest that a Cloud Services RFP to setup a Cloud Framework Agreement is split into 3 lots as below:

- LOT 1 - CLOUD TECHNOLOGIES
  Cloud technologies purchased directly from a CISP or through a designated CISP Reseller.

- LOT 2 – MARKETPLACE
  Access to a marketplace of PaaS & SaaS services.

- LOT 3 - CLOUD CONSULTING
  Cloud-related consulting services (training, professional services, managed services, etc.) and technical support.

*As previously noted, this paper focuses on the purchase of IaaS and PaaS cloud technologies (**LOT 1**) as provided by a CISP (purchased directly from a CISP, or through a CISP Reseller). Separate vendor qualification requirements would be needed for vendors in LOTs 2 and 3 of a cloud services RFP.*

Figure 1 below provides a high-level view of how a well-structured Cloud Services RFP, divided into these three lots, can lead to a Cloud Framework Agreement that provides public sector entities with agility (both technically and contractually), visibility and control of spend and cloud usage, along with the ability to have all of the cloud services necessary to build and maintain the solutions they need.

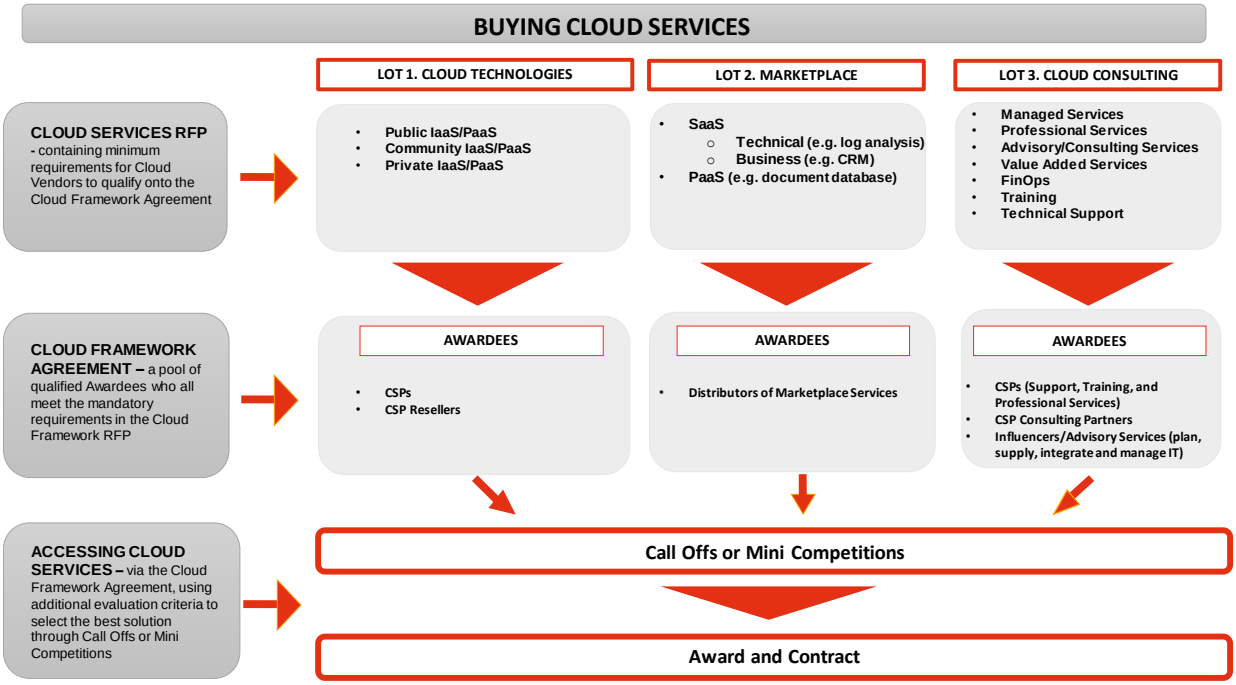

Figure 1 – A successful Cloud Services RFP is separated into 3 lots. Each lot contains Categories or 'types of offering' under the respective lot, to ensure technical and contractual fit to meet end user requirements when purchasing off the Cloud Framework Agreement.

Note that:

- Each lot is multi-award.
- LOT 3 could be awarded via another RFP, or possibly via an existing contract for consulting services.

LOT 1 Categories

Successful Cloud Framework Agreements ask CISPs to describe the model of cloud they are offering, separated into Categories under each lot. We recommend using the industry standard for cloud computing (the National Institute of Standards and Technology (NIST) Essential Cloud Characteristics) – for the definitions of **Public** Cloud, **Community** Cloud, and **Private** Cloud. Structuring a cloud framework agreement this way enables the purchasing agency and public bodies using the framework to pick from a variety of cloud model(s) to suit their needs.

See *Section 2.1.3 Definitions* for the NIST definition of each cloud model under LOT 1 (Public IaaS/PaaS, Community IaaS/PaaS, and Private IaaS/PaaS).

How to Compete – Calls Offs or Mini Competitions?

Qualification criteria for a Cloud Services RFP should cover critical elements and minimum standards, and should not include "nice to have" standards. Adding additional standards above the baseline for vendors qualifying for the framework can lead to some vendors being unable to bid, and ultimately less choice for purchasers.

Following the RFP and subsequent setup of the Cloud Framework Agreement, public sector bodies that are party to the framework can order or 'call off' the cloud services they need when required. Placing a call-off contract under a framework agreement allows buyers to refine requirements with additional functional specification for a call off, whilst retaining the benefits offered under the framework agreement.

If deemed necessary, a mini-competition may be held to identify the best supplier for a particular workload or project. A mini completion is where a customer goes to further competition under the framework agreement, by inviting all suppliers within a lot to respond to a set of requirements. The customer will invite all capable suppliers within the lot to bid, hence the importance of minimum requirements for awardees on a Cloud Services RFP – as it ensures a high standard of options under each lot.

*Note that it is important that there are **distinct sets of T&Cs** of contract for each of the lots as listed in Figure 1 above. A "one-size fits-all approach" to contracting for all lots will lead to issues around technical feasibility and compatibility.*

2.0 Cloud Services RFP Overview

This section describes the Cloud Services RFP model and scope, including: strategic objectives, participants, definitions, timeline, and administrative minimum requirements. Again, we note that the focus of this handbook is LOT 1 - CLOUD TECHNOLOGIES.

2.1 Cloud Services RFP Setup

We strongly recommend public sector entities to be clear as to their high-level objectives and requirements in the Introduction of a Cloud Services RFP.

2.1.1 Introduction and Strategic Objectives

To achieve clarity when it comes to strategic objectives, it is a good practice to articulate in the Introduction of a Cloud Services RFP; **(1)** the business objectives and benefits the organization seeks to achieve by using the cloud; **(2)** the structure of the framework agreement – who buys, who operates, who budgets, etc.; **(3)** a clear understanding of the shared responsibility model between the public sector and cloud vendors, which is at the core of successful cloud purchasing and usage, and **(4)** the type of relationship created between Cloud Service Providers (CISPs), distributors of marketplace services, consulting partners, government procurement/contracting agencies, and government end-users. Articulating these four points helps organizations develop an RFP that best meets their needs, in addition to ensuring that both customers and vendors are clear as to the RFP deliverables.

A Cloud RFP is purposely different from traditional IT RFPs. Cloud technology is not simply a like-for-like replacement for traditional methods of computing - it introduces a completely new way to consume technology. Well-designed Cloud Services RFPs can help public sector entities move quickly to take advantage of the cloud.

Of all the aspects of buying cloud we cite as a good practice, a clear understanding of the shared responsibility model is possibly the best starting point. The shared responsibility model[1] is mostly used when discussing security and compliance in the cloud, but this delineation of responsibilities applies to all aspects of cloud technologies. A Cloud Services RFP should be clear as to what is within a CISP's remit in a cloud environment, and what will remain a customer responsibility. For example, a CISP provides capabilities to monitor resources and applications that run on the cloud, ***but*** it is the customer's responsibility to actually use such CISP-provided capabilities – as a CISP operating at massive scale is not designed do this for millions of customers.

Further, cloud customers should understand how a CISP's Partner Network helps customers utilize the cloud and manage their responsibilities. For example, a cloud Managed Service Provider (MSP) can help a customer configure and use CISP-provided monitoring capabilities to meet their unique compliance and audit requirements.

Simply put, the responsibilities in the cloud model are:

[1] See Section 5 of the CISPE Code of Conduct for Cloud Infrastructure Service Providers: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

A CISP provides cloud technology

A Customer utilizes cloud technology

Consulting firms (if applicable) help a customer access and utilize cloud technology

> ***'Consulting firms'*** *are consulting and managed/professional services firms that help customers design, architect, build, migrate, and manage their workloads and applications on the cloud. Such firms include System Integrators, Strategic Consultancies, Agencies, Managed Service Providers, and Value-Added Resellers.*

Think of 'shopping' for cloud services as analogous to shopping at a hardware store. A vast set of materials and tools to build what you need are available in a hardware store. You can build a cabinet or a swimming pool, or an entire house, it's your choice. When you buy the materials and tools, the hardware store staff can provide guidance and expertise, but they don't come home and build something for you. Therefore, you have a few options:

1. Purchase the materials and tools yourself, and build something yourself.
2. Purchase the materials and tools yourself, and contract someone to build and/or operate something for you.
3. Contract someone to build/operate something for you, and have them provide the materials and tools as part of their overall offering.

If an organization has the in-house skills to build and manage its cloud environment and solutions itself, then it really only needs to access the standardized cloud technologies and tools from the CISP (directly with a CISP, or through a CISP Reseller – see **LOT 1).** SaaS and PaaS software needed should be available on a cloud marketplace (**LOT 2**). If additional consulting, migration, implementation, and/or management help is needed, this is where a CISP's Partner Network comes into play (**LOT 3**).

Sample RFP Language: Introduction and Strategic Objectives

Cloud computing provides public sector organizations with rapid access to a broad range of flexible and low-cost pay-as-you-use IT resources. Organizations can provision the right type and size of resources they need to power their newest bright ideas or operate their IT departments, removing the need for large investments in hardware and/or long term software licensing contracts.

*The **<ORGANIZATION>** has a requirement for access to these types of Commercially Available Cloud Technologies in order to meet its business needs across a broad spectrum of affiliated organizations.*

*The main objective of this RFP is to award non-exclusive parallel **<FRAMEWORK AGREEMENT>** with up to **<x>** providers representing different cloud technologies, and cloud-related services.*

1. ***LOT 1**. Cloud Service Providers (CISPs) or CISP Resellers for the purchase of Cloud Technologies*
2. ***LOT 2.** Providers of marketplace services.*

3. ***LOT 3.*** *Providers of Consulting services to provide additional expertise to migrate to and utilize these CISP offerings*

In respect to ***LOT 1****, bidding organizations (CISPs or CISP resellers) must demonstrate how their offering meets these objectives:*

- ***Agility –*** *Making IT resources available to end-users in minutes instead of the traditional weeks and month's timelines.*
- ***Innovation –*** *Having instant access to the newest and most innovative technology on the market.*
- ***Cost –*** *Trade capital expense for variable expense (e.g.; CapEx to OpEx). Only paying for how much is consumed.*
- ***Budgeting –*** *View billing and usage information at both granular and summary levels, visualizing patterns in spending over time, in addition to forecasting future spend.*
- ***Elasticity –*** *Achieve lower variable costs from the higher economies of scale provided by the cloud.*
- ***Capacity –*** *Eliminate guessing when it comes to infrastructure capacity needs.*
- ***Stop Relying on Data Centres*** *- Focus on the business of our citizens, rather than on the heavy lifting of racking, stacking and powering servers.*
- ***Security –*** *Formalize account design with greater visibility and auditability of resources, and eliminating the cost of protecting facilities and physical hardware.*
- ***Shared Responsibility*** *- Relieve operational burden as the CISP operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates.*
- ***Automation –*** *Build-in automation into cloud architecture to improve the ability to securely scale more rapidly and cost effectively.*
- ***Cloud Governance –*** *(1) start with a full inventory of all IT assets; (2) manage all of these assets centrally; and (3) create alerts regarding usage/billing/security/etc. – all with capabilities for asset tracking, inventory management, change management, log management and analysis, and overall visibility and cloud governance.*
- ***Control –*** *Gain full visibility of how IT services are consumed, and where they can be tuned for security, reliability, performance and cost.*
- ***Reversibility –*** *Portability tools and services to help migrate to and from the CISP infrastructure, minimizing vendor lock-in, and respect of industry Code(s) of Conduct*
- ***Data Protection –*** *Ability to demonstrate compliance with the General Data Protection Regulation (GDPR), through a dedicated industry code of conduct for Cloud Infrastructure services: the CISPE Data Protection Code of Conduct.*
- ***Transparency –*** *Customers should be entitled to know the location of infrastructures used to process and store their data (city area).*
- ***Climate Neutrality –*** *Customers should engage with CISPs that are taking proven, specific steps to meet climate neutrality goals by 2030, and are a signatory of the Climate Neutral Data Centre Pact. This will help Customers to meet their own climate neutrality goals.*

2.1.2 RFP Response Timeline

It is good practice to provide bidders with a timeline of anticipated bid activity when creating a cloud framework agreement, and the associated Cloud Services RFP. The more engagement with industry the better, as it will help ensure that there is a clear understanding by all parties as to the RFP requirements, and indeed of how all vendor services fit into the cloud services model.

Note that the RFP timeline is subject to local laws and legal obligations, and the list provided below is intended as a best practice guide as opposed to a prescriptive list of activities and timeframes.

Sample RFP Language: Response Timeline

See the below RFP timeline for the Cloud Services RFP:

Cloud Services RFP Timeline
• *Request for Information (RFI) Release:* • *RFI Response:* • *Draft Request for Proposal (RFP) Release:* • *Draft RFP Response Due:* • *Industry Consultation Phase: <timelines>* • *Pre-qualification RFP Release:* • *Pre-qualification RFP Response:* • *RFP Release:* • *Round 1 Questions due:* • *Round 1 Answers:* • *Round 2 Questions due:* • *Round 2 Answers:* • *RFP Response Due:* • *Proposal Clarification Period:* • *Negotiation Period:* • *Intent to Award Date:* • *Contract Award:* • *Duration of the Contract (Options to Extend):*

Note that the RFP timeline is subject to local laws and legal obligations, and the list provided below is intended as a best practice guide as opposed to a prescriptive list of activities and timeframes.

2.1.3 Definitions

A Cloud Services RFP should include a detailed list of definitions. This list includes vendor roles (e.g., cloud service provider, cloud reseller, vendor partner), general technology concepts (compute, storage, IaaS/PaaS, SaaS) and other key parts of the agreement. The following is a sample definition list:

Sample RFP Language: Definitions

The below definitions are the National Institute of Standards and Technology (NIST) definitions of cloud computing.[2]

- ***Infrastructure as a Service (IaaS).*** *The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).*

- ***Platform as a Service (PaaS).*** *The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.*

- ***Software as a Service (SaaS).*** *The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.*

- ***Public cloud.*** *The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.*

- ***Community cloud.*** *The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.*

- ***Hybrid cloud.*** *The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).*

- ***Private cloud.*** *The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.*

2.1.4 Detailed Description of the Buying Model and Competing within the Framework Agreement

As noted above, public sector organizations should identify the model for how a framework agreement will operate as a buying mechanism for cloud technologies, and related implementation and management services. This should be made clear in the Cloud Services RFP so that cloud technology vendors, related consulting services organizations, marketplace distributors, and buying entities understand their respective roles.

When it comes to the scope of the framework agreement, and following call-offs or mini competitions, organizations should consider:

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- Who will be responsible for integration and managed services involving the use of the cloud technologies under the contract.
- Is there a requirement for a CISP Reseller/Partner to provide valued added services other than maintaining a contractual relationship with the CISP, providing consolidated billing services, and timely and direct access to usage and billing data associated with usage of the cloud provider services?
- Is there a requirement for a full service value-added reseller, system integrator, or managed services provider, or any form of IT labour services?

It is important to note that a CISP is not a Systems Integrator (SI) or Managed Service Provider (MSP). Many public sector customers will require a CISP for their IaaS/PaaS, and outsource consulting and "hands on keyboard" planning, migration, and management work to an SI or MSP. A depiction of the delineation of the roles and responsibilities in a cloud services model is found below in Figure 2.

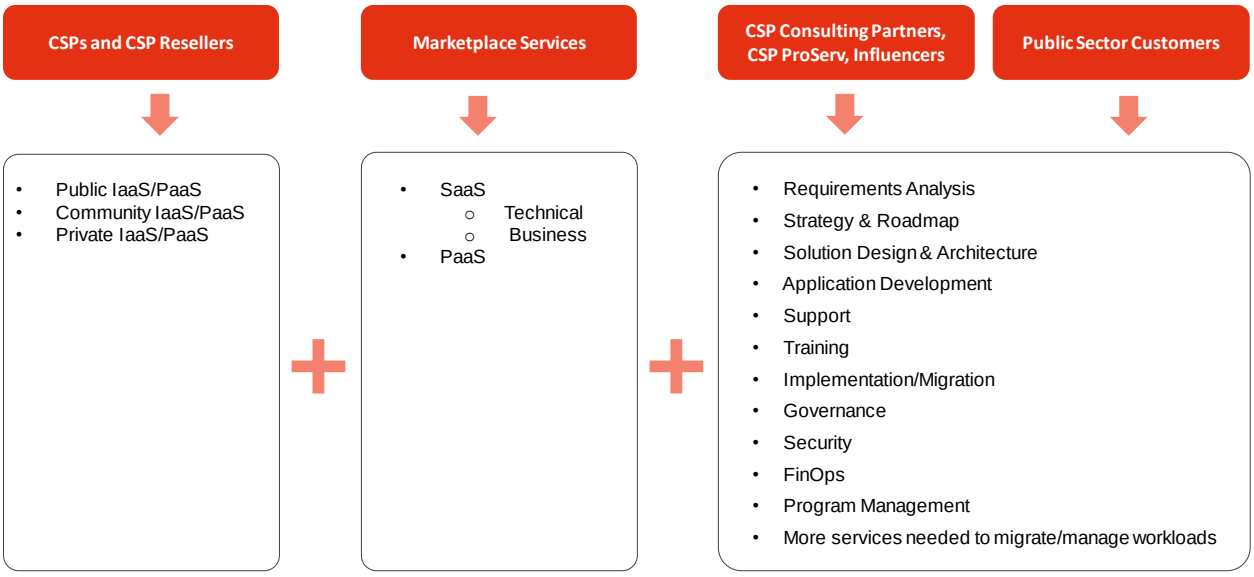

Figure 2 – A Cloud Services RFP should provide end users with a menu of all of the cloud services they need. Public sector customers will require a CISP for cloud technologies, a marketplace for PaaS and SaaS products if needed, then the customer can determine how big a role they want to assume in delivering cloud services and how much they intend to outsource to a Consulting firm/Systems Integrator/Managed Services Provider/etc.

The sample language below is shaped by the roles and responsibilities as shown in Figure 2 above. A Cloud Framework Agreement, and associated Cloud Services RFP, should ensure that buyers are left with the ability to adequately assess each vendor's offerings, allowing them to pick and choose between the services needed for the workload/project. This is best done by separating services into lots as already discussed, and by being clear as to how calls offs and mini competitions are conducted under the framework agreement.

Sample RFP Language: Buying Model

This contract will serve as a ***Framework*** *buying vehicle. This cloud Framework Agreement will include multiple* ***lots*** *as defined by <****ORGANIZATION>****, for Cloud Technologies and related marketplace services/products, consulting services, professional service/system integration/managed service/migration professional services, training and support as defined by <****ORGANIZATION>,*** *and be used by multiple eligible purchasers affiliated with the <****ORGANIZATION****>. This will simplify the procurement process while also optimizing economies of scale.*

Once established, this framework agreement enables an organization to purchase the specific cloud technologies and cloud-related services they want, when they need them—as opposed to purchasing through discrete procurements. Such an approach reduces administrative requirements and significantly reduces procurement complexity and cycle time.

The duration of the Framework Agreement will be maximum ***<X>*** *years including any renewals. The maximum length of a Framework call-off contract is normally* ***<x>*** *months; this can be extended by* ***<x>*** *months and then a further* ***<x>*** *months, with the appropriate internal approvals if needed for contract extension. This will be specified in each specific* ***Call-off.***

The FRAMEWORK is divided into ***3 (three) lots****.*

1. ***LOT 1: CLOUD TECHNOLOGIES*** *- full scope of cloud provider technologies (direct from CISP, from Reseller, or from Reseller with value added services/support):*
    i. ***IaaS and PaaS services*** *– a menu of cloud technologies, e.g. compute, storage, networking, database, analytics, application services, deployment, management, developer, Internet of Things (IoT), etc.). Includes packaged cloud technology solutions such as DR/COOP, Archive, Big Data & Analytics, DevOps, etc.*
2. ***LOT 2: MARKETPLACE*** *– full scope of PaaS and SaaS services/products such as Accounting, CRM, Design, HR, GIS and Mapping, HPC, BI, Content Management, log analysis, etc.*
3. ***LOT 3: CLOUD CONSULTING*** *– full scope of consulting services (managed services, professional services, advisory/consulting services, value added services, FinOps, technical support) related to cloud migration and usage. These services can include: Planning, Design, Migration, Management, Support, QA, Security, Training, etc.*

Vendors can submit their offerings to multiple lots.

Vendors will submit their offerings and related pricing in their format of choice.

COMPETING WITHIN THE FRAMEWORK AND AWARDING CONTRACTS

CALL OFFS

Public sector bodies that are party to the framework agreement can order or 'call off' the services they need when required. Placing a call-off contract under the framework agreement allows buyers to refine requirements with additional functional specification for a call off, whilst retaining the benefits offered under the framework agreement.

Contracts awarded through the framework agreement will be able to show a clear audit trail in terms of the requirements used to select the supplier within each lot. End-purchasers will keep record of communications with vendors, including any early market engagement, clarification questions, emails and face-to-face conversations had.

1. WRITING CALL-OFF REQUIREMENTS AND SEEKING INTERNAL APPROVAL TO BUY

All end-purchasers eligible to use the Framework Agreement will create joint teams of business end users, buying specialists, and technical experts to prepare a list of 'must-haves' and 'wants'. These requirements will help decide which lot(s) are applicable, and which vendor is best qualified to meet requirements. When drafting requirements purchasers will consider:

- *funds available to use the service*
- *technical and procurement requirements of the project*
- *criteria on which the choice will be based*

2. SEARCHING FOR SERVICES

Purchasers under the Framework Agreement will use an online Framework Catalogue (a portal on which Qualified Framework Agreement Awardees and their services will be listed) to find products/services that meet their identified needs. They will choose the appropriate lots, and then search for services.

3. REVIEW AND EVALUATE SERVICES

Purchasers under the Framework Agreement will review service descriptions to find the services that best meet needs based on both requirements and budget. Each service description will include a:

- *Service definition document or links to service definitions*
- *Terms and conditions document*
- *Pricing document (links to public pricing are acceptable with the assumption that a full price list/pricing document, is available on request)*

The price will be the cost of the most common configuration of the service. However, pricing is normally volume-based, so purchasers should always look at the supplier's pricing document or public pricing, and price calculator tools to work out the actual price of what is being purchased, and overall value provided to the buyer (for example, services for optimization and resulting cost reduction).

Purchasers under the Framework Agreement may speak to suppliers to ask them to explain their service description, terms and conditions, pricing or service definition documents/model. A record of any conversations with suppliers will be kept.

4. CHOOSE A SERVICE AND AWARD A CONTRACT

Single Vendor

If only one vendor meets requirements, a contract can be awarded to them.

Multiple Vendors

If there are a number of services on a shortlist, the purchaser will choose the service with the Most Economically Advantageous Tender (MEAT). See the criteria in the following table for the MEAT-based assessment. Purchasers can decide what detailed characteristics to use and how to weight them.

Note that the purchaser may need to:

- *look at combinations of different suppliers*
- *get specific information about volume or enterprise discounts, and vendor cost-optimization services*

Assessment of suppliers should always be fair and transparent. The choice will be based on best fit, and vendors/services will not be excluded without referring back to project requirements.

Table 2 - MEAT Based Assessment

Award criteria
Whole life cost: *cost effectiveness, price and running costs*
Technical merit and functional fit: *coverage, network capacity and performance as specified in relevant service levels*
After-sales service management: *helpdesk, documentation, account management function and assurance of supply of a range of services*
Non-functional characteristics

MINI COMPETITIONS

If deemed necessary, a mini-competition may be held to identify the best supplier for a particular workload or project. A mini completion is where a customer goes to further competition under the framework agreement, by inviting all suppliers within a lot to respond to a set of requirements. The customer will invite all capable suppliers within the lot to bid. See the additional comparison information in the sections below regarding technical, security and pricing/value.

CONTRACT

The buyer and Vendor will both sign a copy of the contract before the service can be used. The maximum length of a Framework contract is normally ***<x>*** *months; this can be extended by* ***<x>*** *months and then a further* ***<x>*** *months, with the appropriate internal approvals if needed for contract extension.*

A copy of the contract must be signed by all interested parties (the buyer and supplier) before the service can be used.

2.1.5 Bidder Minimum Requirements - Administrative

Simple and clear language to set framework agreement qualification criteria will help ensure that there are not submissions from traditional data centre or hardware providers packaging a traditional solution as a 'cloud.' RFP participants should demonstrate how they meet the below minimum bidder administrative requirements.

Again note that this paper focuses on LOT 1 - CLOUD TECHNOLOGIES. However, we have added additional information about LOT 2 - MARKETPLACE and LOT 3 - CLOUD CONSULTING when it helps to provide overall context in terms of requirements and RFP scope. For example, it is important to include minimum qualification criteria for a CISP Reseller/MSP/SI/Consulting firm/etc., and it helps to ensure that they are (1) directly affiliated with the CISP as a reseller or channel partner, (2) certified by a CISP to resell direct access to CISP offerings to third party entities, and (3) have certifications by those CISPs designating their abilities and expertise

Sample RFP Language: Bidder Minimum Requirements – Administrative

This framework agreement will award contracts to multiple vendors in the following categories. Vendors must be a Commercial CISP, a third party reseller of a CISP, a distributor of marketplace services, and/or a provider of services for utilizing a CISP (e.g.; consulting, migration services, managed services, FinOps, etc.). Please identify the roles you are bidding:

LOT 1

____ - Direct provider (CISP) of Public Cloud Service (IaaS AND PaaS)

____ - Direct provider (CISP) of Community Cloud Service (IaaS AND PaaS)

____ - Direct provider of (CISP) Private Cloud Service (IaaS AND PaaS)

____ - CISP Third Party Reseller (ability to provide direct access to a CISPs online cloud offerings).

- *Identify CISP offering that you are able to resell direct access to their service: _____*
- *Provide a letter from the CISP that you are an authorized reseller of their offerings: _____*

LOT 2

____ - Direct provider of Marketplace Services running on a CISP (PaaS and/or SaaS)

____ - Distributor of Marketplace Services running on a CISP (PaaS and/or SaaS)

LOT 3

____ - CISP providing Professional Services

____ - Provider of CISP Technical Support

____- CISP Partner providing services for utilizing or operating on a CISP

____- Influencer/Advisory providing services for utilizing or operating on a CISP

Identify type of offering:

- *Managed Services of workloads on a CISP (Y/N): _____*
  - *Identify Specialties if applicable: _____*
- *Professional Services: (Y/N): _____*
- *Consulting – Training (Y/N): _____*
- *Consulting – Strategy (Y/N): _____*
- *Consulting – Migration (Y/N): _____*
- *Consulting – Cloud Governance (Y/N): _____*
- *Consulting – FinOps (Y.N): _____*
- *Consulting – Other (please identify): _____*

Identify CISP/CISPs you are providing services for: _____
Provide a letter from the CISP confirming your partner designation under the CISPs model: _____

LOT 1 MINIMUM ADMINISTRATIVE REQUIREMENTS

Cloud Service Providers (CISPs)
In order to qualify as a CISP, it must provide conform to the below requirements.

Proposed Qualification Criteria for CISP	*Reason*
Organizational details e.g. Name, Legal structure, Registration/DUNS number, VAT etc.	

Company size, economic and financial standing[3]	*Customer can determine that the CISP will be able to execute on the contract.*
Grounds for exclusion e.g. criminal/fraudulent activities etc.	
Case Studies/ Customer References (specify requisite number/type)	*The customer has the ability to measure CISP experience to deliver the required services.*
Corporate Social Responsibilities	*These should be publicly accessible versions that the CISP provides.*
Publicly available sustainability commitments and practices.	*The customer can see that a CISP is committed to running its business in the most environmentally friendly way possible*
The CISP must provide a proven track record in innovating and releasing new useful services and features over the last 5 years, especially in the field of PAAS, machine learning and analytics, big data, managed services, and cloud-usage optimization features. Publicly accessible changelogs or update feeds can be used to prove the point.	*Demonstrates that the CISP works to get new products into the hands of customers quickly, and then rapidly iterates and improves on products. This helps customers maintain state-of-the-art IT infrastructure without having to make recapitalisation investments*

Reseller/Partner Relationship with CISP

<ORGANIZATION> *requires that the prime contractor be directly affiliated with the CISP as a reseller or channel partner, certified by a CISP to resell direct access to CISP offerings to third party entities, with certifications by those CISPs designating their abilities and expertise. This eliminates the requirement for* ***<ORGANIZATION>*** *to review of the Terms and Services associated with an additional layer of subcontracting between the* ***Framework Agreement*** *prime contractor and CISP. This requirement also reduces the complexity that additional reseller layers generate when (1)* ***<ORGANIZATION>*** *performs its due diligence to ensure clear assignment of responsibilities with regard to the services to be provided, and (2)* ***<ORGANIZATION>*** *executes day-to-day activities involving the consumption of the cloud services*

2.2 Technical

A Cloud Services RFP should raise the bar for CISPs by requiring that they provide the standardized cloud technologies needed for a customer to build their customized solution. As mentioned previously, this difference between what is standardized and what is customized is very important when approaching a Cloud Services RFP. CISPs offer standardized services to millions of customers, so customizations in a Cloud Services RFP focus on higher-up-the-stack solutions and outcomes, as opposed to the underlying methods, infrastructure, or hardware used to offer the cloud services that are used to achieve solution outcomes.

2.2.1 Minimum Requirements

Traditional IT procurements often rely upon business requirements developed through a series of work sessions that document how the organization currently conducts its business. Getting these requirements perfectly right is a difficult process in the best of circumstances. If successful, these requirement sessions document the historic business process that may, in itself, be antiquated and inefficient. If those requirements are then made a part of the RFP to be replicated by the CISP, the only solution may be a custom-made solution. This model is incompatible with cloud procurements.

[3] Note that a Cloud Services RFP looks to high level company information, as opposed the number of employees in the company and internal employee team structure. With cloud technology there is no correlation between guarantee of service performance, and number of employees. Instead, cloud RFPs look to overall company size to meet requirements (adequate scale) and proven experience/performance.

Public sector organizations should understand their business objectives and performance needs, but should not be prescriptive in an RFP in that they dictate the system design and functionality. Instead, the organization should be shopping for the best business fit. Rather than evaluate proposals on hundreds or even thousands of prescriptive requirements that may not lead to successful services, organizations should include evaluation criteria based on how well the technology and associated services will meet or enhances business objectives, whether it achieves their performance needs, and the ability to fine-tune business rules through configuration.

Cloud RFPs should ask the right questions in order to obtain the best solutions. Given that in a cloud model physical assets are not being purchased, it follows that many traditional data centre procurement requirements are not applicable. ***Recycling data centre questions will inevitably lead to data centre answers****, which results in CISPs being unable to bid, or leads to poorly designed contracts that hinder public sector customers from extracting the full capabilities and benefits of the cloud.*

A Cloud Services RFP focuses on the key requirements required of a CISP and cloud services, ensuring that vendors that qualify for LOT 1 meet a high-bar. The requirements should also avoid being too prescriptive, so as not to limit public sector access to a broad range of qualified CISPs.

Sample RFP Language: Cloud Provider Capabilities

Also see the above minimum CISP administrative requirements for LOT 1

Proposed Qualification Criteria for CISP	*Reason*
Infrastructure	
The CISP infrastructure should offer at least 2 clusters of datacentres. Each cluster must be comprised of at least 2 datacentres connected by low latency link to allow for Highly Available Active-Active deployments and implementations of DR-BC scenarios. The datacentres comprising each cluster must be physically isolated and failure-independent from each other.	*The CISP needs to be able to offer an infrastructure apt to build highly available applications where single points of failure can be avoided.*
CISP should provide logically and geographically isolated regions. Customer Data must not be replicated outside these regions by the CISP.	*Data residency requirements mandate that the customer is in full control of where their data is located.*
The CISP must have the ability to deliver direct, dedicated and private connectivity between the CISP datacentres.	*Private connectivity is a fundamental requirement to be able to build a hybrid, secure infrastructure.*
CISP should provide sufficient mechanisms, which include encryption for data in transit.	*The customer can require that there is a capability that no data can transit unencrypted.*
Minimum CISP certifications	
The CISP must be certified ISO 27001	*Third party auditing, certification and accreditation ensures customers can benchmark services (and in particular the platform) for quality, safety and reliability. It is essential that a minimum of certifications are met.*

The CISP must be compliant with the CISPE Data Protection Code of Conduct, in order to provide features and services that can be used in compliance with the GDPR, which allow customers to build GDPR compliant applications.	*The customer must be able to build or run applications in compliance with GDPR.*
The CISP must make available 3rd-party audited reports such as SOC 1 and 2 Reports (covering the locations and services used by EC) to allow transparency with respect to the CISP controls and procedures.	*The CISP needs to be transparent as to how the application is operated and managed. SOC reports are instrumental to ensuring trust and transparency*
The CISP must be adherent to the Climate Neutral Data Centre Pact	*The Climate Neutral Data Centre Pact engages the CISP to reach Climate Neutrality by 2030, and therefore enable the user to support its own sustainability goals. Third party auditors are mandatory for providers >250 FTE (non SMEs)*
The CISP must be adherent to SWIPO IaaS Portability Code of Conduct	*The SWIPO IaaS Portability Code of Conduct ensures that services meet the requirements of the Art. 6 "Data Porting" of the Free Flow of non-personal Data Regulation.*
Service Characteristics	
The CISP infrastructure must be accessible through programmatic interfaces (APIs) and web based management console.	*Self-service access and programmatic interfaces are a required standard of CISP providers to disintermediate as much as possible user access and the provider itself.*
The CISP must offer a foundation set of Services including: Object Storage, Managed Relational Database, Managed Non-Relational Database, Managed Load Balancers, Monitoring and integrated Autoscaling.	*The mere offer of virtual machines is not sufficient to qualify a provider as a cloud provider. Cloud providers should offer a set of PAAS and IAAS services to accelerate and improve customer's applications.*
The CISP must allow the Customer to freely change their services usage and configuration, or move data within and outside the CISP (self-service offering).	*Self-service access to services and data is a hard requirement that allows the customer to be fully independent.*
The CISP must allow for "pay per use" billing of their services.	*Pay per use allows the customer to cost-optimize its workloads, minimize risk and leverage the CISP for short-lived applications and PoCs.*
Data and Systems Security	
The CISP must allow the Customer to retain full control of their data, give the Customer freedom to choose where data is stored (city urban area), and guarantee that no customer data will be moved unless such move is initiated by the Customer itself.	*The customer must have control over where data is stored, how to manage access to content, and user access to services and resources*
The CISP characteristics must give the Customer full control of their security policies, including Confidentiality, Integrity, and Availability of the Customer data and systems.	*The customer must be able to define and implement its security standards across its workloads. Trusting the provider to "do the right thing" with customer's data is not enough.*
Cost Control	
The CISP must have mechanisms and tools to allow the customer to monitor spending over time. Tools must allow for basic segmentation of cost based on workload, service and account.	

The CISP must offer tools to alert the customer whenever a cost threshold is surpassed.	
The CISP must deliver detailed bills to the customer. It must be possible to structure the bill to break cost by workload, environment and account.	

CISP's should also provide responses to the technical requirement questions below.

SOLUTIONS

CISP should demonstrate how it can provide pre-built templates and software solutions that are either hosted on or integrate with the CISP, for the following solutions:

- *Storage*
- *DevOps*
- *Security/Compliance*
- *Big data/Analytics*
- *Business Applications*
- *Telecommunications & Networking*
- *Geospatial*
- *IoT*
- *[Other]*

Provide an overview of how the CISP has been used for the following workloads:

- *Disaster Recovery*
- *Dev and Test*
- *Archiving*
- *Backup and Recovery*
- *Big Data*
- *High Performance Computing (HPC)*
- *Internet of Things (IoT)*
- *Websites*
- *Serverless Computing*
- *DevOps*
- *Content Delivery*
- *[Other]*

2.2.2 Comparison between Vendors

In addition to the minimum requirements in a Cloud Services RFP, it is important to provide criteria by which CISP technologies can be compared during a competitive evaluation.

Cloud Services RFPs should ask for those cloud capabilities an organization needs, with an understanding that the customer owns using such capabilities to build their solution. Functionality beyond the standard that a CISP can provide (such as pre-built solutions via the CISP, or automation features) - can be used for a more meaningful analysis of "value-added options" or "best value" in a Cloud Services RFP.

The public sector often requires competition between bidders using evaluation criteria like best value, most economical advantageous tender (MEAT), or lowest price. As public sector entities plan for this portion of a Cloud Services RFP, it is important to build an approach that takes into account the unique features of cloud. For example, understand that simply comparing line items between cloud providers' offerings (e.g.; compute or storage) is not an effective way to compare offerings. Instead, we strongly recommend a focus

on higher-level solutions such as those listed above in section *2.2.1*. Public sector entities can then look to cloud-specific requirements, such as those listed in *Appendix A – Technical Requirements for Comparison between Bidders*.

RFPs should state the essential cloud characteristics needed to build its cloud solution. To do this, public sector organizations can leverage the National Institute of Standards and Technology (NIST) Essential Cloud Characteristics, in addition to using third party analysts' reports for ensuring the CISP has the best fit 'true cloud' offering, that operates at massive scale.

Sample RFP Language – Comparison between Vendors

*CISP's should provide responses to ALL technical requirement questions in **Appendix A**.*

Respondents must have the following attributes and must describe how their offers of cloud services meet the five essential characteristics for cloud computing[4].

1) ***On-Demand Self Service:*** *Respondent must provide the capability to unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider. The Respondent shall provide the capability for the ordering activity to unilaterally (i.e.; without vendor review or approval) provision services. Explain how this works with your offering or the offer you are representing.*

2) ***Ubiquitous Network Access:*** *Respondent must provide multiple network connectivity options, one of which must be Internet-based. Explain how this works with your offering or the offer you are representing.*

3) ***Resource Pooling:*** *The respondent's CISP must provide pooled computing resources that serve multiple consumers using a multi-tenant model with different virtual resources dynamically assigned and reassigned according to consumer demand. The user is able to specify location at a higher level of abstraction (e.g.; country, region or data centre location). The respondent shall support scaling of these resources within minutes or hours of a provisioning request. Explain how this works with your offering or the offer you are representing.*

4) ***Rapid Elasticity:*** *The respondent's CISP shall support service provisioning and de-provisioning capabilities (scale up and down), making the service available within minimum prescribed times (maximum 'x' hours) of the provisioning request. The respondent shall support billing adjustments resulting from these provisioning requests on a daily basis on an hourly or daily basis.*

5) ***Measured Service:*** *The Respondent shall offer visibility into service usage via an online dashboard or similar electronic means.*

In addition, the CISP must:

- *Be a recognized leader in providing cloud services as demonstrated by the Gartner Magic Quadrant for IaaS[5]*
- *Provide industry-recognized third-party analyst reports that demonstrate the CISPs proven capabilities and reliability.*

Finally, CISPs will be compared using the scenarios given in Appendix B.

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

2.2.2.1 Service Level Agreements (SLAs)

CISPs provide standardized commercial SLAs to millions of customers, and are therefore not able to offer customized SLAs, as is the case in an on-premises data-centre model. However, CISP customers (often assisted by CISP Partners) can architect their cloud usage to leverage a CISP's commercial SLAs to meet and exceed customer-specific requirements and unique SLAs.

Cloud Services RFPs should ensure that CISPs offer the capabilities and guidance needed to leverage their services and commercial SLAs, so that individual end users can meet performance and availability requirements.

Sample RFP Language: Service Level Agreements

Provide information on, and links to the CISPs approach to Service Level Agreements (SLAs).

***<ORGANIZATION>** will maintain awareness of CISP SLAs and deploy important workloads and applications in such a way that they continue to operate in the event an SLA is not met.*

***<ORGANIZATION>** will be responsible for maintaining appropriate SLA's associated with any **<ORGANIZATION>** owned equipment or **<ORGANIZATION>** operated services used with the CISP.*

*The CISP should provide **<ORGANIZATION>** with the capabilities to have ongoing visibility and reporting of its operational SLA performance, and documented best practices to leverage CISP infrastructure to architect services for performance, durability and reliability.*

2.2.3 Contracting

CISP terms and conditions are designed to reflect how a cloud services model functions (physical assets are not being purchased, and CISPs operate at massive scale offering standardized services); thus it is critical that a CISP's terms and conditions are incorporated and utilized to the fullest extent practicable. See section *2.5* below for more information on terms and conditions, and contracting.

2.2.3.1 New and Changing Services

CISPs are providing performance through a service. Unlike traditional on-premises solutions that require upgrades and service maintenance contracts that expire, cloud providers simply provide the standardized service. For the cloud model to achieve economies of scale, upgrades and changes to underlying infrastructure are rolled out to all, not to individual users, and customers then pick and choose the services they use. The service is more seamless than on-premises systems of the past, and cloud providers constantly add new and enhanced services for customers to use as they wish.

If new or enhanced CISP services cannot be added after an RFP submission deadline, public sector organizations restrict themselves from being able to avail of new services and enhanced features until the next iteration of a Framework Agreement is released. We therefore strongly recommend that the provision of the services described within the Framework Agreement is broad permitting the addition of new CISP services after the submission deadline. EU procurement law may restrict the introduction of materially different new CISP Services to be added to the Framework Agreement but updates and new versions of services which are not deemed material changes could be added without any procurement challenge.

Sample RFP Language: New and Changing Services

*The CISP shall provide a cost effective solution that utilizes both proven and stable virtualization technologies and cutting edge technologies constantly refreshed. The **<ORGANIZATION>** acknowledges and agrees that the Cloud Technologies may be provided on a shared service basis to the **<ORGANIZATION>** and other clients of the CISP from a common code base and/or common Environment and the CISP may from time to time: change add or delete the functions, features, performance, or other characteristics of the Cloud Services, and if such change, addition or deletion is made, the specifications of the Cloud Service shall be amended accordingly.*

*The scope of this delivery order includes all currently existing and, new or enhanced CISP Services **WITHIN THE SCOPE OF THE FRAMEWORK**. CISP provided cloud services available to commercial customers shall be made available to **<ORGANIZATION>**.*

2.2.3.2 Vendor Lock-in/Reversibility

Cloud technology reduces vendor lock-in as physical assets are not being purchased, and customers can move their data from one cloud provider to another at any time.

However, some degree of vendor lock-in is inevitable when purchasing cloud services – as not all clouds are equal, and therefore one CISP may offer services and capabilities that another simple cannot provide – therefore reducing the ability to use such services with another provider. A prudent approach is to require that CISPs provide the requisite features and services to exit their cloud, with documentation as to how to use these services serving as a reasonable 'exit strategy' – given that it is impossible for a CISP to know the unique configuration of a customer's use of their standardized services, and as such provide a customized exit plan.

See section 2.3.1.2 for information on Industry Codes of Conduct to address "Data Porting" and "Switching Cloud Providers" to fulfil requirements of Article 6 of the EU "Free Flow of non-personal Data Regulation".

Sample RFP Language: On-Boarding and Off-Boarding

*The **<ORGANIZATION>** is seeking proposals that provide a reasonable exit strategy to prevent lock-in. The **<ORGANIZATION>** is not buying physical assets, and the CISP will provide the ability to move up the IT stack and move down it again. The CISP will provide portability tools and services to help migrate to and from the CISP platform, minimizing lock-in. Detailed documentation as to how to use CISP-provided portability tools and services will serve as a reasonable exit plan.*

*The CISP should not have **required** minimum commitments or **required** long-term contracts.*

*Data stored with a service provider can be exported by customer at any time. The CISP shall allow the **<ORGANIZATION>** to move data as needed on and off CISP storage. The CISP shall also allow virtual machine images to be downloaded and ported to a new cloud provider. The **<ORGANIZATION>** can export its machine images and use them on-premises or at another provider (subject to software licensing restrictions).*

2.3 Security

Security and compliance responsibilities are shared between a CISP and cloud customers. In this model, cloud customers control how they architect and secure their applications and data put on the infrastructure, while CISPs are responsible for providing services on a highly secure and controlled platform, and for providing a wide array of additional security features. The level of CISP and customer responsibilities in this model depends on the cloud deployment model (IaaS/PaaS/SaaS) and customers should be clear as to their responsibilities in each model.

Understanding this shared responsibility model is crucial to devising a successful Cloud Services RFP. Public sector organizations should ensure they know what a CISP is responsible for, what they themselves are responsible for, and where consulting/ISVs partners and their solutions fit-in to help.

2.3.1 Minimum Requirements

The key word when it comes to security in the cloud is **Capability**. Public sector organizations should be demanding of CISPs, requiring that CISPs provide the security capabilities needed to ensure that customers can meet their responsibilities in the shared responsibility model. As seen from the representative requirement list below, the CISP is asked to provide a standardized capability, so that the customer can utilize it to make their unique cloud environment secure.

- ***Provide*** *network firewalls and web application firewall* ***capabilities*** *to create private networks, and control access to instances and applications.*
- ***Provide*** *connectivity* ***options*** *that enable private, or dedicated, connections from your office or on-premises environment.*
- ***Provide*** *the* ***capability*** *to implement a defence in depth strategy and thwart DDoS attacks.*
- *Data encryption* ***capabilities*** *available in storage and database services.*
- ***Provide*** *flexible key management* ***options****, allowing you to choose whether to have the CISP manage the encryption keys or enable the customer to keep complete control over keys.*
- ***Provide APIs*** *for customers to integrate encryption and data protection with any of the services developed or deployed in a CISP environment.*
- ***Provide*** *deployment* ***tools*** *to manage the creation and decommissioning of CISP resources according to organization standards.*
- ***Provide*** *inventory and configuration management* ***tools*** *that identify CISP resources and then track and manage changes to those resources over time.*
- ***Provide tools and features*** *that enable customers to see exactly what's happening in their CISP environment.*
- ***Enable*** *deep* ***visibility*** *into API calls - including who, what, who, and from where calls were made.*
- ***Provide*** *log aggregation* ***options****, streamlining investigations and compliance reporting.*
- *Provide capability to configure alert notifications when specific events occur or thresholds are exceeded*
- ***Provide capabilities*** *to define, enforce, and manage user access policies across CISP services.*
- ***Provide*** *the* ***capability*** *to define individual user accounts with permissions across CISP resources*
- ***Provide*** *the* ***capability*** *to integrate and federate with corporate directories to reduce administrative overhead and improve end-user experience.*

More of these requirements are found in *Appendix A – Technical Requirements for Comparison between Bidders*.

Functionality beyond the minimum standard for security can be used for a more meaningful analysis of "value-added options" or "best value" in an RFP. And the more functionality that is built-in or automated when it comes to security, the better. Again, see *Appendix A – Technical Requirements for Comparison between Bidders* for requirements for comparison between bidders.

Public sector organizations should look to cloud accreditation certifications and evaluations for assurance that the required CISP security controls are in place. For example: consider a CISP that has been validated and certified by an independent auditor to confirm alignment with ISO 27001 certification standard. ISO 27001 Annex A, domain 14 digs into the specific controls that a CISP adheres to according to ISO requirements around system acquisition, development and maintenance. It is likely that these controls cover the majority, if not all, of the controls around system acquisition, development and maintenance that would usually be asked by an organization in an IT-related RFP. Therefore, it makes sense that an

organization simply requires that a CISP is ISO 27001 certified, instead of duplicating effort and listing control requirements around system acquisition, development and maintenance in a Cloud Services RFP.

This approach of leveraging third party compliance reports can be applied to most security and compliance controls, for example: CISPE GDPR Code of Conduct, ISO, SOC, etc.

Sample RFP Language: Security

*The CISP shall disclose its non-proprietary security processes and technical limitations to the **<ORGANIZATION>** such that adequate protection and flexibility can be attained between the **<ORGANIZATION>** and the service provider.*

The CISP shall state its roles and responsibilities when it comes to security and compliance:

- *Describe security-related roles and responsibilities of the CISP and **<ORGANIZATION>** in the proposed offering. Be clear as to the delineation of responsibilities, and outline CISP services to aid **<ORGANIZATION>** in building and automating security functions in its cloud environment.*
- *Provide responses to the technical specifications in **APPENDIX A** related to **<ORGANIZATION'S>** security requirements.*

OWNERSHIP AND CONTROL OF <ORGANIZATION> CONTENT

*Describe how CISP capabilities can protect the **<ORGANIZATION'S>** data privacy. Include the controls in place to address the protection of **<ORGANIZATION'S>** content. CISP must provide strong regional isolation, so that objects stored in a region never leave the region unless the **<ORGANIZATION>** explicitly transfers them to another region*

- *The **<ORGANIZATION>** will manage access to its content, services and resources. The CISP should provide an advanced set of access, encryption, and logging features to help **<ORGANIZATION>** do this effectively. The CISP will not access or use **<ORGANIZATION'S>** content for any purpose other than as legally required and for maintaining the CISP services and providing them to **<ORGANIZATION>** and its end users.*
- *The **<ORGANIZATION>** will choose the region(s) in which its content will be stored. CISP will not move or replicate the **<ORGANIZATION'S>** content outside of its chosen region(s), except as legally required and as necessary to maintain the CISP services and provide them to the **<ORGANIZATION>** and its end users.*
- *The **<ORGANIZATION>** will choose how its content is secured. CISP must provide strong encryption for **<ORGANIZATION'S>** content in transit or at rest, and provide the option for the **<ORGANIZATION>** to manage its own encryption keys.*
- *CISP must have a security assurance program using global privacy and data protection best practices in order to the **<ORGANIZATION>** establish, operate and leverage the CISP's security control environment. Security protections and control processes must be independently validated by multiple third-party independent assessments*

Cloud accreditation certifications and evaluations provide public sector organizations with assurance that CISPs have effective physical and logical security controls in place. When these accreditations are leveraged in RFPs, it streamlines the procurement process, and helps to avoid duplicative, overly burdensome processes or approval workflows that may not be required for a cloud environment.

Cloud RFPs should provide CISPs with an opportunity to prove that they align with compliance accreditations and evaluations. As mentioned above, there is a considerable overlap in risk scenarios and risk management practices across these accreditation schemes, and as controls and requirements are bundled together in such accreditations, requiring that CISPs comply with accreditations is a quicker way to address compliance in an RFP rather than duplicating the effort in listing such individual controls (many

of which may be taken from previous RFPs that are directly at on-premises data centres, and as such may not apply to cloud computing).

NOTE: it is also very important to understand how the reports listed below can be accessed. For example, SOC 1 and SOC 2 reports are typically sensitive documents. Understand the agreements needed to access them (e.g.; non-disclosure agreement – NDA) and do not simply ask for those documents to be submitted as part of the RFP response (those documents could be made public through Open Records acts or similar legislation jeopardizing cloud security).

Sample RFP Language: Compliance

The use of recognized security, compliance and operational standards, derived from best practices in cloud service operations — including data handling, data security, confidentiality, availability, etc. — streamline the procurement of cloud technology.

The <ORGANIZATION> will evaluate unique proposal offerings against accepted security, compliance and operational standards as outlined below and in Appendix A. By relying on the vendor's certification of compliance against each standard, the <ORGANIZATION> can use minimum compliance against the standard as the baseline for evaluation of the proposal.

Requiring the CISP to continue compliance with the minimum standard over the life of the contract provides the benefit of keeping the service-compliance current.

The CISP that is being bid (directly or through a reseller) should be able to demonstrate its ability to meet the following independent third-party attestations, reports and certifications (Note – if some of these attestations, reports and certifications are under disclosure restrictions due to security issues, the <Organization> will work with the CISP to obtain jointly agreed upon access):

Certifications / Attestations	*Laws, Regulations, and Privacy*	*Alignments / Frameworks*
☐ C5 (Germany)		*☐ CDSA*
☐ CISPE Data Protection Code of Conduct (GDPR)		
☐ CNDCP (Climate Neutral Data Centre Pact)		
☐ DIACAP	*☐ EU Data Protection Directive*	*☐ CIS*
☐ DoD SRG Levels 2 & 4	*☐ EU Model Clauses*	*☐ Criminal Justice Info. Service (CJIS)*
☐ HDS (France, Healthcare)		
☐ FedRAMP	*☐ FERPA*	*☐ CSA*
☐ FIPS 140-2	*☐ GDPR*	*☐ EU-US Privacy Shield*
☐ ISO 9001	*☐ GLBA*	*☐ EU Safe Harbor*
☐ ISO 27001	*☐ HIPAA*	*☐ FISC*
☐ ISO 27017	*☐ HITECH*	*☐ FISMA*

☐ *ISO 27018*	☐ *IRS 1075*	☐ *G-Cloud [UK]*
☐ *IRAP [Australia]*	☐ *ITAR*	☐ *GxP (FDA CFR 21 Part 11)*
☐ *MTCS Tier 3 [Singapore]*	☐ *PDPA – 2010 [Malaysia]*	☐ *ICREA*
☐ *PCI DSS Level 1*	☐ *PDPA – 2012 [Singapore]*	☐ *IT Grundschutz [Germany]*
☐ *SEC Rule 17-a-4(f)*	☐ *PIPEDA [Canada]*	☐ *MARS – E*
☐ *SecNumCloud (France)*		
☐ *SOC1 / ISAE 3402*	☐ *Privacy Act [Australia]*	☐ *MITA 3.0*
☐ *SOC2 / SOC3*	☐ *Privacy Act [New Zealand]*	☐ *MPAA*
☐ *SWIPO IaaS Code*		
	☐ *Spanish DPA Authorization*	☐ *NIST*
	☐ *U.K. DPA - 1988*	☐ *Uptime Institute Tiers*
	☐ *VPAT/Section 508*	☐ *UK Cloud Security Principles*

The list above has been provided for illustrative purposes only and should not be considered exhaustive of the certifications and standards that could apply to Cloud Services.

2.3.1.1 Data Protection

A key consideration when using cloud services is that the processing of personal data is carried out in accordance with applicable EU data protection law, including the General Data Protection Regulation (GDPR). GDPR is a principle-based regulation and therefore does not provide sector-specific guidance to help ensure compliance. However, GDPR encourages the adoption of compliance tools such as codes of conduct to provide such guidance. CISPE, working with the French Data Protection Authority (CNIL) has developed a data protection code of conduct (CISPE Code[6]) endorsed by the European Data Protection Board with a general applicability in Europe. The purpose of the Code is to help CISPs comply with GDPR and guide customers in assessing whether CISPs are suitable for the processing of personal data that the customer wishes to perform.

- The Code focuses exclusively on the IaaS sector and addresses the specific roles and responsibilities of IaaS providers.
- It helps to clarify the aspects of fair and transparent processing and appropriate security measures in the context of cloud infrastructure services (GDPR, Article 40 [2]).
- It helps customers understand how they can retain sovereignty over their data by ensuring that it remains within the EU.
- It promotes data protection best practices that support the EU's GAIA-X initiative to develop European cloud data services.

[6] https://cispe.cloud/code-of-conduct/

CISP compliance with data protection codes of conduct such as the CISPE Code provide assurance that personal data will be processed in strict compliance with GDPR.

Sample RFP Language: Data Protection

The CISP that is being bid (directly or through a reseller) should be able to demonstrate its ability to comply with a data protection code of conduct such as the CISPE Code. The data protection code must align with the requirements laid out in the GDPR framework. The code should include at a minimum; (1) a clear definition of roles and responsibilities of the CISP, (2) the requirement that the CISP will not use customer data for marketing or advertising purposes, and (3) the ability for customers to select CISP services that allow data to be processed entirely within the European Economic Area. Compliance with the code must be verified by external independent auditors (monitoring bodies) accredited by independent, external auditors accredited by the European Data Protection Authority.

2.3.1.2 Switching Cloud Providers and Porting Data

Customers should have the freedom to choose the cloud services they want to use, and not be 'locked in' by a CISP or PaaS/SaaS provider.

CISP-provided cloud services are standardized and offered on a "one to many" basis, with services configured, provisioned and controlled by the customer. A benefit of cloud computing is that customers have the ability to choose whatever standardized services they need to develop their unique applications and solutions. This benefit extends to being able to switch to new or different services that best meet customer needs at any particular time.

As with data protection, codes of conduct can help provide customers with assurance and confidence when it comes to switching to the cloud from on-premises infrastructure, or when switching between CISPs. Together with EuroCIO (the European Association of CIOs), CISPE co-chaired to the development of the code of conduct for data portability and cloud service switching for IaaS cloud services (SWIPO IaaS Code[7,8]). The first version of the code was developed in accordance with the EU Free flow of Data Regulation, handed over to the European Commission in November 2019 under the EU Finnish Presidency and published by the association SWIPO AISBL in May 2020. In April 2021 the first services were declared in adherence to the code by SWIPO AISBL, and in May 2021 the first CISPE member services were declared to adhere to the code.

Sample RFP Language: Switching Cloud Providers and Porting Data

The CISP that is being bid (directly or through a reseller) should be able to demonstrate its ability to comply with a 'switching and data porting' code of conduct such as the SWIPO IaaS Code. The code must detail how a CISP offers customers' safe transfer of business data, should they decide to switch from a CISP.

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security

[8] https://swipo.eu/

2.3.2 Comparison between Vendors

As with the technical criteria in the sections above, in addition to the minimum security requirements in a Cloud Services RFP, it is important to provide criteria by which CISP security capabilities and services can be compared during a competitive evaluation.

See *Appendix A – Technical Requirements for Comparison between Bidders* for sample CISP security requirements. We strongly recommend that the below capabilities are key security considerations for public sector entities evaluating CISPs:

Sample RFP Language: Key Security Considerations

- *CISP understanding of the shared responsibility model, and documentation to help customers understand the delineation of security responsibilities for CISP features and service (for example, in the context of GDPR)*
- *Proven history of CISP infrastructure security, with publicly available non- proprietary documentation of CISP security posture and physical/logical controls*
- *CISP Support specific to cloud security*
- *Services that enable customers to formalize account design, automate security and cloud governance controls, and streamline auditing*
- *The capability to create, provision, and manage a collection of resources in a template-like fashion (includes CISP/CISP-Partner built gold-standard security templates)*
- *The capability to establish reliable and repeatable operation of controls*
- *Features for continuous and real-time auditing*
- *The capability for technical scripting of cloud governance policies*
- *The capability to create forcing functions that cannot be overridden by users who aren't allowed to modify those functions*
- *The ability to execute reliable implementation of what was previously written in policies, standards and regulations, along with creating enforceable security and compliance, which in turn creates a functional reliable cloud governance model for IT environments*
- *Services to protect from common, most frequently occurring network and transport layer distributed denial of service (DDoS) attacks, along with the ability to write customized rules to mitigate sophisticated application layer attacks*
- *Managed threat detection service*

2.3.3 Contracting

As noted above, CISP terms and conditions are designed to reflect how a cloud services model functions (physical assets are not being purchased, and CISPs operate at massive scale offering standardized services); thus it is critical that a CISP's terms and conditions are incorporated and utilized to the fullest extent practicable. See section *2.5* below for more information on terms and conditions, and contracting.

When it comes to security, we again strongly recommend allowing CISPs to constantly update offerings, or that suppliers be allowed to add products after the submission deadline, so long as they conform to the original parameters of the RFP**.** This reflects the fact that security features and services evolve quickly, and CISPs release security-focused services often, that are in many cases free to use. Note that it is important to have a baseline security level (see the minimum requirements above) so as to guarantee that changes to security offerings will not be detrimental.

The shared responsibility model is of course at the core of security in a Cloud Services RFP. Each party needs to be clear as to their security responsibilities, and CISPs should be required to document CISP/Customer

security responsibilities for CISP-provided cloud technologies, along with documentation to help customers build-in and automate security best practices.

A cloud Framework Agreement should provide flexibility to remove a vendor should they no longer comply with the minimum security and compliance requirements as set out in the Cloud Services RFP.

2.4 Pricing

To contract for cloud technology in a manner that accounts for fluctuating demand, public sector organizations need a contract that lets them pay for services as they are consumed – with the required cloud governance and visibility around usage and spending.

Importantly, Cloud Services RFPs should look at value and total cost of ownership (TCO), as opposed to simple apples-to-apples comparison of unit prices. This traditional practice of looking to the lowest unit price does not translate to the cloud model, and as such does not tend to lead to most economical advantageous tender, or overall lowest price.

*To aide CISP pricing evaluation, it helps to first have CISP pre-qualification or shortlisting, with **minimum pricing-related requirements** so that CISPs with similar capabilities can qualify for the framework agreement. The evaluation process for call offs and mini competitions can then look to a selection of typical example cloud architectures and **pricing scenarios** that match some typical public sector workloads, and have CISPs price them. Live Test Demos are also recommended to allow for comparison of performance and elasticity of cloud technologies services provided by CISPs. See Appendix B for a sample demonstration test script for cloud technologies.*

2.4.1 Minimum Requirements

The pricing section in a Cloud Services RFP has four key elements:

1. **Utility Pricing:** Cloud customers are incorporating a pay-as-you-go utility model, where at the end of each month they simply pay for their usage, which is optimal for utilization and resource metrics.
2. **Transparent Pricing:** CISP pricing should be publicly available and transparent.
3. **Dynamic Pricing:** Include the flexibility to allow cloud prices to fluctuate based on market pricing. This approach takes advantage of the dynamic and competitive nature of cloud pricing, and supports innovation and price reductions.
4. **Controlled Spending:** CISPs should provide reporting, monitoring, and forecasting tools that allow customers to (1) monitor usage and spend at both summary and granular levels, (2) get alerts as to when usage and spend hit custom thresholds, and (3) to estimate usage and spend in order to plan future cloud budgets.

Sample RFP Language: Pricing

*The **<ORGANIZATION>** requests that responding CISPs include their proposed method and pricing model for providing each of their services to end users as a commercial cloud capability.*

The CISP shall provide:

- *Service definition document or links to service definitions*
- *Terms and conditions document*
- *Pricing document (links to public pricing are acceptable, with the assumption that a full price list/pricing document, is available on request)*

The price will be the cost of the most common configuration of the service. CISPs should provide options for volume-based discounts, and price calculator tools to work out the actual price of what is being purchased, and overall value provided to the buyer (for example, services for optimization and resulting cost reduction).

Purchasers under the Framework Agreement may speak to suppliers to ask them to explain their service description, terms and conditions, pricing or service definition documents/model. A record of any conversations with suppliers will be kept.

Additional Pricing Requirements

- *Provide cloud technologies with a dynamic pricing model that gives maximum business flexibility and allows for scalability and growth.*

- *Pricing attributes must include the following:*
  - *Is pricing provided in an on-demand, utility-style, pay-as-you-go service? Explain your pricing model.*
  - *Can you achieve further discounts when committing to usage and/or buying in bulk? Provide details on how.*
  - *Is pricing publicly available and transparent? Please include links to publicly available pricing.*
  - *Is pricing dynamic and responds quickly and efficiently to market competition?*
  - *Do you provide best practices and resources to track spending?*
  - *Do you provide best practices and resources for cost optimization?*

Pricing Transparency

*Due to the constant downward pricing trend in commercial cloud technologies driven by innovation and competition, the metered CISP service unit cost paid by the **<ORGANIZATION>** under the Framework Agreement shall never exceed the cloud provider unit pricing published on the cloud provider Website that is effective at the time the unit of service is consumed by customer.*

Budgeting and Billing Alerts/Reports

*To demonstrate delivery and use of cloud technologies, CISPs should provide **<ORGANIZATION>** with the tools to generate detailed billing reports that break down costs by the hour, day, or month; by each account in an organization; by product or product resource; or by customer-defined tags. **<ORGANIZATION>** recognizes that as part of the cloud shared responsibility model, **<ORGANIZATION>** will be responsible for using CISP-provided budgeting and billing features and tools to meet unique forecasting and reporting requirements.*

- *Provide information as to how **<ORGANIZATION>** can view billing information at both granular and summary levels, visualizing patterns in spending on CISP resources over time, in addition to forecasting future spend.*

- *Provide information as to how **<ORGANIZATION>** can filter usage/billing view by service, by linked account, or by custom tags applied to resources, and create billing alerts that send notifications when usage of services approaches or exceeds <**ORGANIZATION**>-defined thresholds/budgets.*

- *Provide information as to how **<ORGANIZATION>** can forecast how much cloud services it use over a defined forecast time period, based on past usage. CISP should offer an **estimate** of what **<ORGANIZATION'S>** CISP bill will be, and enables **<ORGANIZATION>** to use alarms and budgets for amounts that it is predicted to use, in order to have greater governance over cost and spending.*

2.4.2 Comparison between Vendors

Public sector organizations often require competition between bidders using evaluation criteria like best value, most economical advantageous tender (MEAT), or lowest price. When planning for the pricing of framework agreement call offs or mini competitions, it is important to build an approach that takes into account the unique features of cloud. For example, understand that simply comparing line items between cloud providers' offerings (e.g.; compute or storage) is not an effective way to compare as it does not take into account features like performance, cost optimization using cloud-native services and CISP monitoring tools, or differentiating services that CISPs may offer for free. Additionally, the catalogue price of a CISP can be tens of thousands of line items, the pricing models differ from one service to another and one provider to another.

Analyse TCO

We recommend to focus on the total cost of ownership (TCO) of defined use cases, which take into account all aspects of a cloud solution (including partner services, standardized CISP discounts, technical features that can increase performance, and reduce/optimize costs, etc.).

Compare by Scenarios

The evaluation process can also consider the typical scenarios that correspond to common systems or applications. Such scenarios (things like web hosting, or the implementation of a human resources system with x number of users, etc.) can include variables such as the speed and scale of the resources, performance of the application or solution, storage access times, low volume complex data compared to simple computing tasks with high volume, etc. The applications or systems can also have typical scenarios such as processing of high volume when the tax return, emergency notifications such as flood warnings. The scenarios should be comprehensive to include the scope of technology and services that the customer may use during the project. This way, the customer is able to compare the estimated overall cost of the project.

Compare Scenarios Financially and Technically

It is also important to take into account technical advantages when comparing pricing between CISP offerings. For example, one CISP may enable allows customers to build an active-active Disaster Recovery (DR) topology thanks to its model of having data centres in clusters within a geographical region. A CISP who does not have this kind of redundancy and data centre configuration could be x% more expensive given the cost of factoring-in disaster recovery needs. As an example of why a holistic approach to pricing that includes additional technical features is crucial to evaluating CISPs, consider the below alternative of a straight 'apples to apples' comparison.

Example: A customer wants to compare the price of object storage provided by qualified CISPs on a framework agreement. The price of the item of the storage 'unit' from CISP 1 is € 0.023/GB. The price of the same 'unit' CISP 2 is € 0.01 GB. In a simple unit to unit comparison, the customer would not ask critical questions such as:

1. How many redundant copies of the object are available in case of failure? In the above example, CISP 1 is designed to sustain the concurrent loss of data in two different facilities and maintains multiple copies of data. In the case of CISP 2, redundant copies are not made.
2. What is the level of sustainability of stored objects? CISP 1 is 99.999999999%, CISP 2 is 99%.

3. Take into account the cost over the life of ownership of the overall project or workload, and how cost optimization features can reduce costs when it comes to how data is stored and used (for example, increasing the use of Serverless functions of a CISP can reduce costs by x%.

These are just some of many other technical considerations that factor into pricing, particularly related to security and compliance.

Considerations for pricing scenarios include

Base rates – these are essentially public prices of CISPs. CISPs should provide these prices publicly; however, as noted above to effectively compare CISPs, customers can ask for perhaps 3-5 specific scenarios (or however many makes sense for the customer) to be priced by all vendors. Scenarios should be comprehensive to include the breadth of services and technologies that the customer is likely to use during the course of the project. This way the customer is able to compare the overall estimated cost of the project. Comparisons made at the line-item/SKU level tend to be more problematic than helpful to customers and vendors (customers would have to compare tens of thousands of line items across all CISPs, and vendors would have to provide this level of detail and manage it when the actual price is only determined based on service consumption).

Evaluating a CISP's overarching capability-set is a must for cloud customers looking to get best value. For example, CISPs may have a number of services that are either free or essentially free, and a pricing evaluation should take such services into account, and that other CISPs may charge for similar functionalitv..

Evaluation criteria can be written in such a way that allows the CISPs to call out their "included x default" features, and how such services have on overall impact cost. Evaluation criteria can also look to CISP volume based/tiered pricing and commercially available discounts such as Reserved Instances/Spot Instances. For example:

- x% saving if customers purchase reserved compute capacity (1yr, 3 yr, etc.)
- x% discount on tied/volume pricing
- x% saving based on architecture reviews and optimisation of infrastructure such as switching to the better fit compute option
- As noted above, take into account whole life cost, and how cost optimization features can reduce cost

PRICING SCENARIO
Bidders must provide pricing for the below scenario only for evaluation purposes. The actual price will be based on consumption of services on an on-demand pay-per-use model.

Below are representative requirements for the purpose of price discovery and are provided with the explicit understanding that during the duration of the contract these nominal requirements will change. Please provide pricing for both 12 & 36 months on-demand and 12 & 36 months reserved capacity.

Provide:

- *Name of proposed solution(s):*

- *Bidder's best pricing:*

- *Service Hours: 24x7x365*
- *Service Availability: 99.95%*

Pricing scenarios can also include examples from existing customers with similar workloads who have optimised their spend over 1/2/3 years - though using CISP monitoring and optimisation tools, adopting optimised cloud native solutions, and through CISP price reductions.

2.5 Contract Execution Setup/T&Cs

CISP provided cloud technologies and operations are standardized by-design, therefore the contractual conditions are standardized as well. However, there is an ability to marginally adjust these contracts to adapt to local legislative and regulatory contexts.

Often traditional IT procurement methods include strict rules that require the applicants to comply with many or all requirements of the procurement or be rejected. Or they perhaps include a strict subset of mandatory requirements. When this kind of sourcing method is used with cloud technologies, which are really a set of standardized components and tools that help you architect a custom solution, procurements tend to fail.

2.5.1 Terms and Conditions

The first step when it comes to contracting in a Cloud Services RFP is to review and understand existing CISP commercial terms which, in many cases, can be found publicly on CISP websites. Public sector entities are increasingly comfortable accepting commercial terms from CISPs. Part of this effort to understand terms is to meet with CISPs and their partners to dive deep on their approaches. The key question to ask is 'why' do CISPs operate with specific terms. Some of these terms may seem different to traditional IT terms, but there are very specific reasons 'why' they are part of a cloud contract. If the publicly available terms are not acceptable, CISPs often have slightly modifiable agreements for enterprise customers that can be explored.

Along with reviewing the CISP's terms & conditions, it is important to understand existing policies, regulations and/or laws (e.g.; those involving technology, data classification, privacy, personnel, etc.). Oftentimes there are existing policies/regulations/laws that are designed for buying and utilizing traditional IT offerings, and they can be at odds with a CISP's model. For example, only allowing the use of cloud technologies that were included in the original Framework Agreement bid via the Cloud Services RFP. CISPs are constantly adding new services and adding new features. Stifling access to those new services simply because you are following a traditional IT product refresh approach makes no sense for the end customer. If this is the case, it is important to have in-depth discussions with CISPs that include looking at these policies/regulations and/or laws.

Take Advantage of Pre RFP Discussions

As stated above, before drafting a RFP, take the time to meet with CISPs and related vendors to understand their terms & conditions and to educate them on your entity's approach, policies, regulations and laws. The most important part of these discussions is for both sides to learn 'why' the relevant terms work the way they do. For example, cloud terms & conditions are different from traditional data centre, managed service, hardware, shrink-wrapped software and system integration terms. Because they are single models and

involve constant innovation, their business models require the RFP process to be sufficiently flexible to allow for negotiations or discussions to receive clarification.

By including the ability to clarify terms and conditions throughout discussions or negotiations, public sector organizations gain greater understanding of cloud models and avoid the problem of rejecting providers that actually might be able to meet the organization's needs. One typical process is for the organization to identify certain terms in advance that it is willing to discuss and negotiate before award. By negotiating acceptable terms with the bidder(s) in advance, the organization ensures it is getting the best fit for the award and resolves differences that otherwise might result in the rejection of an effective proposal. Public sector entities can also review their policies, regulations and laws, and both sides can gain an understanding of how using the cloud will fit into those models. Often times, there are ways to work with the existing clauses. However, if there is an area that is problematic, both teams can work together to find a solution (it is better to have these discussions well before any RFP and follow-on contractual negotiation).

Negotiation Flexibility

To be able to sign contracts in compliance with local legislation, while relying on standardized contractual terms by CISP, it is recommended (1) to request from applicants their standard contract, (2) not to enact unsuitable contractual conditions when setting up the framework agreement for the Cloud Services RFP, and (3) provide a negotiation option on all of the provisions of the consultation and proposals that will result in the framework agreement (except, of course, the obligatory clauses mandated by law).

NB: the scope of shared responsibility is inherent in the cloud model and should be reflected in the terms of the contract (e.g. the CISP confirms that customers own their data, where it resides, and provides tools to ensure that the choice of data locations is limited - **BUT** - it is the responsibility of the customer or partner to use these tools.

*Note that it is important that there are **distinct sets of T&Cs** of contract for each of the LOTs in a Cloud Framework Agreement. A "one-size fits-all approach" to contracting for all LOTs will lead to issues around technical feasibility and compatibility.*

As already noted, RFPs that include mandatory terms that are not negotiable are essentially a "take it or leave it" proposition for providers that can cause an otherwise acceptable proposal to be rejected. Public sector organizations should carefully consider the consequences of using mandatory terms **unless it is a requirement of law**. Organizations should be certain about the need for a mandatory requirement or term because future negotiations are pre-empted by their classification as mandatory. The use of mandatory requirements or terms should be kept to an absolute minimum, to provide the organization with the flexibility needed to acquire the best technology and solution.

Keep in mind that CISP cloud technologies are completely standardized and delivered in a fully automated way. Therefore, a CISP is not able to make any kind of change to terms and conditions that would require any underlying service customization. Furthermore, the prices of the services are typically public and standardized for all users, which means that a CISP cannot adjust pricing in order to absorb more risk on behalf of a particular customer.

Indirect Purchases

An alternative option to purchasing cloud technologies directly from a CISP is to purchase them from a CISP reseller instead. More information on CISP Resellers is found in section *2.1.3* above.

Sample RFP Language: Terms and Conditions

*CISPs or representative vendors must provide their publicly available terms & conditions and provide feedback on key terms & conditions provided by the <**ORGANIZATION**>.*

*<**ORGANIZATION**> intends to enter into a written contract with the successful bidder based on the bidder's contractual terms. The bidder should provide a set of proposed contractual terms for <**ORGANIZATION**> to review, which represents its best commercial and legal proposal. Offerors and the <ORGANIZATION> can discuss both sets of terms & conditions during the <DISCUSSION/NEGOTIATION> phase.*

- *High-level Framework Head Terms would consist at most of the following components:*
  - *Framework duration*
  - *Framework governance*
  - *Framework performance*
  - *Framework termination*
  - *Scope of the Framework*
  - *Ordering Process*
  - *Confidentiality provisions*
  - *Category specific IP and information*
  - *Minimum technical requirements to be met by CISPs – e.g. quality standards, accreditation, security and data protection*
- ***There will be different terms for each of the Framework Agreement lots***
- *CISP service specifics can be considered and will be dealt with at the call off*
- *Allow contract changes – the terms should not constrain customers and suppliers to agree contract changes, to bolt on new services or enhancements. The evolving nature of cloud services is such that service enhancements will become available on an on-going basis all of which can help deliver efficiencies to customers*
- *Service Level Agreements (SLAs) should not be specified by the customer. Customer terms should not define commission specific, bespoke SLAs that differ from CISPs standard service delivery models. Allowing CISPs standard SLAs, CISPs will be able to keep cost low and pass these onto customers whilst allowing customers to be confident that the CISP can meet the SLA.*
- *Liability caps should be proportionate. Liability should be proportionate to the services that are purchased and there should not be disproportionately high liability caps. If caps are disproportionately high this would act as a disincentive for CISPs to accept low value projects. These projects often act as a useful introduction and "test" case for customers to determine whether certain cloud solutions are effective for their organization.*
- *Customers should own their own data. Customers should control and own their data and have the ability to determine the geographic location in which it is held. This will allow customers to avoid vendor lock-in and move data to new providers freely.*

2.5.2 Software Terms and Conditions

Although this handbook focuses on the purchase of IaaS and PaaS cloud technologies as provided by a CISP, it is important to highlight software terms and conditions that public sector organizations can consider when purchasing software from vendors. Please refer to Figure 1 (Page 5) to review how software is purchased as part of a well-structured Cloud Services RFP.

Software plays a critical role in almost every business, including public sector. Including obligations such as Software Licensing Terms and Conditions in a Cloud Services RFP helps to ensure that Public Sector entities receive best value and have freedom to choose vendors when purchasing software.

See the Ten Principles of Fair Software Licensing for Cloud Customers[9] for more information. The Principles have been developed by Cigref[10] an association of major French companies and public administrations representing the users of digital technology, in collaboration with CISPE, and the support of other European trade associations of CIOs and Providers, to address practices that both associations see as harming the digital transformation of organizations of all sizes as they move to the cloud.

Sample RFP Language: Software

*<**ORGANIZATION**> intends to enter into a written contract with the successful bidder based on the bidder's contractual terms. The bidder should provide a set of proposed contractual terms for <**ORGANIZATION**> to review, which represents its best commercial and legal proposal. Software Vendors and the <ORGANIZATION> can discuss both sets of terms & conditions during the <DISCUSSION/NEGOTIATION> phase.*

***Requirement 1.0.** Software vendors must provide clear licensing terms, including a breakdown of costs at summary and granular levels.* ***Requirement 1.1.** All charges relating to any failure to comply with license terms must be provided at summary and granular levels.*
***Requirement 2.0.** Software licences must provide <Organization> the ability to migrate the licensed software from on-premises to the cloud of their choice, without requiring the purchase of separate, duplicative licences for the same software.* ***Requirement 2.1.** Software licenses must be free from licensing restrictions and increased costs that restrict <Organization's> ability to run the licensed software in the cloud of their choice.*
***Requirement 3.0.** Software Licences must permit <Organization> to run the licensed software on their own hardware (typically referred to as "on-premises" software) as well as on the cloud of their choice.*
***Requirement 4.0.** Software licenses must not require that the licensed software only run on hardware dedicated solely to <Organization>.*
***Requirement 5.0.** Software vendors must not penalize <Organization> if the vendors' licensed software is used on another supplier's cloud offering, for example by including rights to undertake increased or intrusive software audits, or impose higher software licensing fees.*
***Requirement 6.0.** Directory software must support open standards for syncing and authenticating user identities in a non-discriminatory way with other identity services.*
***Requirement 7.0.** Software vendors must not charge different prices for the same software based solely on who owns the hardware on which it is installed.*

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

Requirement 7.1. *Prices for software must not discriminate between software installed in <Organization's> own data centre, a data centre managed by a third party, on computers leased from a third party, or in the cloud provider of <Organization's> choosing.*
Requirement 8.0. *During the term of the contract, software vendors must not make material changes to licence terms that restrict <Organization> from previously permitted uses, unless required by law or due to security concerns.*
Requirement 9.0. *Software vendors must not mislead <Organization> by representing that software licences will cover <Organization's> intended software use as outlined in the <Organization's Requirements>, when covering such use may require the purchase of additional licences.*
Requirement 10.0. *Should <Organization> have the right to resell and transfer software licences, software vendors must continue to offer support and patches under fair terms to <Organization> who has lawfully acquired a resold licence.*

2.5.3 How to Select Between Awardees per Project

Public sector bodies that are party to the framework can order or 'call off' the services they need when required. Placing a call-off contract under a framework agreement allows buyers to refine requirements with additional functional specification for a call off, whilst retaining the benefits offered under the framework agreement.

If deemed necessary, a mini-competition may be held to identify the best supplier for a particular workload or project. A mini completion is where a customer goes to further competition under the framework, by inviting all suppliers within a lot to respond to a set of requirements. The customer will invite all capable suppliers within the lot to bid, hence the importance of minimum requirements for awardees on a Cloud Services RFP – as it ensures a high standard of options under each lot.

Again note that it is important that there are distinct sets of T&Cs of contract for each of the lot categories of Type of Offering (e.g. Public IaaS/PaaS, Community IaaS/PaaS, Private IaaS/PaaS), as a "one-size fits-all approach" to contracting for each lot will lead to issues around technical feasibility and compatibility.

See section *2.1.4* for sample RFP language when it comes to selecting between Awardees.

2.5.4 On-Boarding and Off-boarding

One consideration to keep in mind when setting up a Cloud Framework Agreement is the option of a Dynamic Purchasing System (DPS). With a DPS model, all vendors who meet the minimum requirements for the Framework Agreement will be admitted to the Framework. There is no hard limit on the number of vendors that may join the Framework, and unlike the traditional framework model, vendors can also apply to join the 'DPS Framework' at any point during its lifetime.

We strongly recommend public sector entities to set standards high to ensure quality and assurance of service from qualified vendors, but not to be too specific as to disqualify CISPs in a manner that does not ensure fair competition. Ultimately the goal is to avoid saturating the end user with a vast number of options, while keeping the standard of cloud technologies available high.

3.0 Best Practices/Lessons Learned

Below we highlight some lessons learned as to how to realize a successful Cloud Framework Agreement with a well-written Cloud Services RFP.

3.1 Cloud Governance

Governance in the cloud is a shared responsibility. CISPs provide features and services to build-in cloud governance into every aspect of a cloud environment, while customers bring their existing cloud governance standards and learn how the cloud is a cloud governance enabler.

In the cloud, customers get the chance to build the IT environment they want, not simply manage the one they have. The cloud enables customers to: (1) start with a full inventory of all IT assets; (2) manage all of these assets centrally; and (3) create alerts regarding usage/billing/security/etc. All of these vital benefits of the cloud help customers have an optimised—and to the fullest extent, automated—architecture, with no need to continually procure and install new hardware. This is done by the CISP, allowing customers to shift focus from undifferentiated infrastructure management to the mission-critical operational level.

One helpful way to view a CISP cloud is that it is effectively a very large API. Whether you are launching a new server or changing a security setting, you are just making API calls. Every change to the environment is logged and recorded (the who, what, where, and when of each change is recorded). This provides cloud governance, control, and visibility that is only possible in a cloud environment. It allows customers to rethink their existing IT governance models, and determine how they can be streamlined and improved given the benefits that the cloud brings.

Cloud governance can also mean communicating and incorporating the positive process changes and new skill sets that come with the cloud. For example, project managers are familiar with waiting months for an IT environment to be built out, and as such could significantly over-estimate schedules for creating a development or test environment in the cloud (which with the cloud can take mere minutes). Adapting to this new-found agility will be an evolutionary process and happens program by program. Such lessons learned should be shared so that a Cloud Framework Agreement can continue to evolve in such a way that requirements are the right fit for new processes and agility.

3.2 Budgeting for Cloud

When it comes to how to structure pay-as-you-use cloud pricing to fit with public sector acquisition and budgeting requirements, we have found that it helps to bundle CISP services into a single line item (compute, storage, networking, database, IoT, etc.), all under a line item of Cloud Technologies. This approach provides flexibility to offer all current and new CISP technologies to users in real time, and provides users with quick access to the resources they need, when they need them. It also accommodates fluctuating demand, leading to optimized utilization and low costs.

Public sector organizations can add additional line items for orders from other lots on a cloud framework, should they require consulting/professional or managed services, software from a marketplace, cloud support services, and training on CISP's offerings.

Additional contracting flexibility can be provided by employing optional contract line items within appropriate resource categories to accommodate future growth. Alternatively, if an organization wanted

to bundle Cloud Technologies with consulting/professional/managed services into one line item, it can be done so with a line item such as "Cloud Technologies and Ancillary Labour."

Below is a representative example of this approach. In the below example, each unit of the line item '#1001 - Cloud Technologies, equates to €1.00 of "Cloud Technologies" used. Each month, ordering increments can be funded based on current and forecasted usage projections.

Table 3 - Example Single Line Item Pricing Structure.

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001	Cloud Technologies	1,000	Each	€1	€1,000
1002	Consulting Services	1	Per Week	€3,000	€3,000
1003	Cloud Support	1	Per Month	€1,000	€1,000
1004	Cloud Training	1	Per Day	€3,00	€3,000
1005	Cloud Marketplace	10	Each	€10	€100

As an example of how this structure can work: A public sector organization engages with a CISP to estimate how much cloud technology services the organization is going to use. The organization agrees to terms with the vendor such as €10 million over 5 years, which comes to €2 million per year. The organization commits the initial €2 million annual amount. Each month there is a bill and the money is taken from the fund to pay it. There is a drawdown against that account. The remaining funds are monitored for burn rate using CISP monitoring and forecasting tools. If the remaining funds get low, the organization requests additional funds from the CFO that can be committed to maintain services.

Sample RFP Language: Pricing - Contracting

PAYMENT TERMS

The payment terms have to be structured accordingly to pay only for the resources used by the <ORGANIZATION> as indicated below:

1. *Monthly Payment to be based on actual usage/consumption of services and as per the CISPs publically available pricing.*

MINIMUM GUARANTEE AND MAXIMUM SPEND

Because it will be impossible for the <ORGANIZATION> to determine exactly what volume of a specific Cloud Service Provider's resources will be consumed over a period of time, orders will be specified as fixed price unit quantities of a single ordering line item for "Cloud Technologies.

Each unit of the line item ordered will equate to <€1.00> worth of Cloud Technologies ordered. Incremental orders will be periodically placed via modification to this order in various quantities to provide <ORGANIZATION> with the flexibility to pre-order various "euro amount" quantities of CISP Cloud Technologies based on its estimated usage for needs of varying duration. Quantities will be periodically pre-ordered by <ORGANIZATION> in amounts sufficient to cover the estimated cost for cloud technologies that will be used to meet a variety of requirements.

Item No.	Description	Qty	Unit	Price
01	CISP Cloud Technologies	1,000	EA	€1,000.00

MINIMUM ORDER/INCREMENTAL ORDER
Orders will be placed periodically for various quantities of <10.000> line item units based on the <ORGANIZATION'S> estimated usage of cloud technologies. This arrangement will provide the <ORGANIZATION> with the flexibility to pre-order <10,000> units of "Cloud Technologies" as necessary to support operations and to remain consistent with cloud computing "pay as you go" commercial practices."

An initial increment of <100,000> units at cost of <€100.000> will be ordered when the call-off is placed. The minimum number of total line item units that can be placed on a single incremental order using one or more line items is <x>. The maximum number of units that can be ordered under the delivery order cannot exceed <x>, but is subject to never exceeding the call-off value when combined with all previous units ordered. <ORGANIZATION> will be responsible for ensuring all orders are within the limits specified in this section.

ORDER MAXIMUM
The total maximum order value is up to <x> consisting of up to < x> units of a single line item priced at <x> per unit. The value is based on an estimate of <ORGANIZATION'S> requirements over the period of performance, but is not guaranteed.

3.3 Understand Partner Business Model

Public sector entities should seek to understand the models under which CISPs provide their offerings and recognize that partners providing consulting, managed services, reselling and much more are critical to the process. Many customers require a cloud provider for their infrastructure, and outsource "hands on keyboard" planning, migration, and management work to a Systems Integrator (SI) or managed services provider. Given this mix of 'services', there may be requirements that are not applicable to cloud providers, such as a flow-down clauses to subcontractors.

Taking such flow-down clauses to illustrate why it is important to understand how partners and resellers operate in relation to CISPs, in some procurement types there are clauses that require the prime contractor to flow-down certain mandatory clauses to all of its partners/subcontractors. Typically, CISPs will not provide or bid as formal subcontracting partners as they offer a standardized service at a massive scale that is not tailored to fit a particular end customer's unique requirements (including the needs of a public sector customer under a public sector contract). In an indirect procurement model (procuring cloud services through a CISP Reseller), a CISP may reject these clauses from its reseller as not applicable to a "2nd tier" supplier of commercial services. In such a case, the CISP is not itself performing the scope of work under the contract; rather, a CISP partner is using CISP infrastructure to do so. The CISP is therefore a commercial supplier (not a subcontractor) to a partner's operations. In a direct procurement model (buying cloud services directly from a CISP), a CISP would typically reject these "mandatory" clauses appropriate for a typical commodity subcontractor due to the commercial nature of the contracted services, and the fact that most CISPs do not require subcontractors to supply their commercial services.

3.4 Cloud Brokers

The concept of a Cloud Broker as a means to reduce the possibility of vendor lock-in can be problematic. Although a cloud broker may be a sound idea in theory, in practice it would likely introduce more complexity and confusion than realized value.

Trying to architect applications to work across multiple clouds simultaneously or interchangeably inevitably leads to trade-offs in capability (there is no Rosetta stone for the cloud). This approach can ultimately add an unnecessary layer of complexity between public sector customers and their cloud services, which can

compromise the efficiencies and security gains it seeks to attain—leading to reduced scalability and agility, increased costs, and decelerating innovation.

3.5 Pre-RFP Sourcing/market research

As a public sector entity plans for a Cloud Services RFP, it should the include stakeholders from all aspects of the organization – senior leadership, the business stakeholders, technology, finance, procurement, legal, and contracts – from the very beginning of the process. This approach ensures that all stakeholders have an understanding of the cloud model, and consequently an educated approach to reassessing traditional IT procurement methods.

With it comes to dialogue with industry, we strongly recommend public sector entities to take time to have in-depth conversations to gather feedback from industry – CISPs, CISP Partners, PaaS/SaaS Marketplace vendors, and industry experts. For example, such dialogue can take the form of industry days or security and procurement workshops. Another effective way to gain a deep understanding of cloud procurement is to release an RFI, or ideally a draft RFP document. Often they include potential issues that can be identified, discussed and adjusted before the finalised Cloud Services RFP is released.

3.6 Sustainability

Sustainability is inherent in cloud computing and moving to the cloud provides an energy efficiency gain, when compared to on-premises servers or enterprise data centres. Identifying a CISP that prioritizes sustainability and has made public commitments to achieve sustainability goals provides further assurance that the cloud is sustainable. European CISPs and data centre operators (with the support of the European Commission) created the Climate Neutral Data Centre Pact[11], a Self-Regulatory Initiative to establish clear, simple and far-reaching sustainability criteria for the data centre industry and ensure that data centre operators and cloud service providers are climate neutral by 2030. The Self-Regulatory Initiative includes clear targets for data centre energy efficiency, water conservation, server reuse and repair, and the use of carbon-free energy to power data centres. CISPs that sign-up for the Self-Regulatory Initiative agree to meet these targets and certify against the criteria to be considered a climate neutral operator.

A Cloud Services RFP should ask CISPs if they have committed to such criteria, specifically asking whether they have signed up for self-regulation and when they took on such a commitment.

Sample RFP Language: Sustainability

Have you committed to operate climate neutral data centres by signing onto the Climate Neutral Data Centre Self-Regulatory Initiative? If so, when did you become a signatory?

Can you provide evidence that you have been awarded the Climate Neutral Data Centre Pact seal for use?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

Appendix A – Technical Requirements for Comparison between Bidders

Below we list some generic cloud technology requirements that could be used to compare CISPs during Call Offs or Mini Competitions on a Cloud Framework Agreement.

1. Cloud provider profile

	Requirement
1.	***MARKET EXPERIENCE:*** *How many years has the cloud provider been operating in the cloud market segment?*
2.	***OPENNESS AND DATA PROTECTION:*** *Does the cloud provider adhere to Data Protection or Reversibility industry Codes of Conduct? Does the cloud provider adhere to open source and open API development principles?*

2. Global infrastructure

	Requirement
1.	***GLOBAL REACH:*** *Does the cloud provider offer a global infrastructure to help users achieve low latency and high throughput?*
2.	***REGIONS:*** *Does the cloud provider have a regional presence in the geographies needed?*
3.	***DOMAINS/ZONES:*** *Does the cloud provider implement the concept of domains or zones, where multiple data centres are grouped through a low-latency network to provide a higher degree of high-availability and fault tolerance?* • *If yes, please list the number of domains or zones and the number of data centres within the needed geography*
4.	***DOMAINS/ZONES DISTANCE:*** *Does the cloud provider build its domains or zones with data centres that are located physically apart to support redundancy, high-availability, and low latency?*
5.	***DATA CENTERS BUILT:*** *Does the cloud provider offer data centres engineered to be isolated from failures in other data centres, with redundant power, cooling, and networking?*
6.	***DATA CENTER REPLICATION:*** *Does the cloud provider offer data replication across data centres within a domain or zone with automatic failover?*
7.	***DOMAIN/ZONE REPLICATION:*** *Does the cloud provider offer data replication across domains or zones within a region?*

3. Infrastructure

3.1 Compute

	Requirement
1.	***COMPUTE – REGULAR INSTANCE – GENERAL PURPOSE:*** *Does the cloud provider offer the following instance types?* • *General purpose – optimized for generic applications and provides a balance of compute, memory, and network resources.* ○ *If yes, what is the largest instance?*
2.	***COMPUTE – REGULAR INSTANCE – MEMORY-OPTIMIZED:*** *Does the cloud provider offer the following instance types?* • *Memory optimized – optimized for memory-intensive applications* ○ *If yes, what is the largest instance?*
3.	***COMPUTE – REGULAR INSTANCE – COMPUTE-OPTIMIZED:*** *Does the cloud provider offer the following instance types?* • *Compute optimized – optimized for compute-intensive applications* ○ *If yes, what is the largest instance?*
4.	***COMPUTE – REGULAR INSTANCE – STORAGE-OPTIMIZED:*** *Does the cloud provider offer the following instance types?* • *Storage optimized – offers a large amount of local storage capacity* ○ *If yes, what is the maximum storage capacity (i.e. 5,10,20,50 TB) and the maximum number of disks (HDDs/SSDs) that can be provisioned and attached to an instance?*
5.	***COMPUTE – REGULAR INSTANCE – GRAPHICS-OPTIMIZED:*** *Does the cloud provider offer the following instance types?* • *Low-cost graphics – offers low-cost graphics acceleration to compute instances?* ○ *If yes, what is the largest instance?*
6.	***COMPUTE – REGULAR INSTANCE – GPU-OPTIMIZED:*** *Does the cloud provider offer the following instance types?* • *GPU – offers hardware graphic processing units (GPUs) for graphic-intensive applications* ○ *If yes, how many GPUs and what GPU models is the cloud provider able to offer per instance?*
7.	***COMPUTE – REGULAR INSTANCE – FPGA-OPTIMIZED:*** *Does the cloud provider offer the following instance types?* • *FPGA – offers field programmable gate arrays (FPGA) for developing and deploying custom hardware acceleration for applications.* ○ *If yes, how many FPGAs is the cloud provider able to offer per instance?*
8.	***COMPUTE – BURSTABLE INSTANCE:*** *Does the cloud provider offer burstable instances that provide a baseline level of central processing unit (CPU) performance with the ability to burst above the baseline?*

	• *If yes, what is the largest burstable instance?*
9.	*COMPUTE – IO-INTENSIVE INSTANCE:* *Does the cloud provider offer instances that use non-volatile memory express (NVMe) solid state drives (SSDs) optimized for low latency, very high random I/O performance, and high sequential read throughput?* • *If yes, what is the maximum input/output operations per second (IOPS) capacity of the largest instance?*
10.	*COMPUTE – TEMPORARY LOCAL STORAGE:* *Does the cloud provider support local storage for compute instances to be used for temporary storage of information that changes frequently?*
11.	*COMPUTE – MULTIPLE NIC SUPPORT:* *Does the cloud provider support multiple (primary and additional) network interfaces cards (NICs) to be allocated for a given instance?* • *If yes, what is the maximum number of NICs per instance?*
12.	*COMPUTE – INSTANCE AFFINITY:* *Does the cloud provider offer users the capability to logically group instances together within the same data centre?*
13.	*COMPUTE – INSTANCE ANTI-AFFINITY:* *Does the cloud provider offer users the capability to logically group instances and place them in different data centres within a region?*
14.	*COMPUTE – SELF-SERVICE PROVISIONING:* *Does the cloud provider offer self-service provisioning of multiple instances concurrently either through a programmatic interface, a management console, or a web portal?*
15.	*COMPUTE – CUSTOMIZATION:* *Does the cloud provider offer customizable instances, i.e., ability to modify configuration settings such as virtual central processing units (vCPUs) and random access memory (RAM)?*
16.	*COMPUTE – TENANCY:* *Does the cloud provider offer single tenant instances that run on hardware dedicated to a single user?* • *If yes, what is the largest available single-tenant instance?*
17.	*COMPUTE – HOST AFFINITY:* *Does the cloud provider offer the ability to launch an instance and specify that this instance always restarts on the same physical host?*
18.	*COMPUTE – HOST ANTI-AFFINITY:* *Does the cloud provider offer the capability of splitting and hosting specific instances across different physical hosts?*
19.	*COMPUTE – AUTOMATIC SCALING:* *Does the cloud provider offer the ability to automatically increase the number of instances during demand spikes to maintain performance (i.e. 'scale-out')?*
20.	*COMPUTE – IMAGE IMPORTING MECHANISM:* *Does the cloud provider offer users the ability to import their existing images and save them as new, privately available images that can then be used to provision instances in the future?* • *If yes, what formats are supported?*
21.	*COMPUTE – IMAGE EXPORTING MECHANISM:* *Does the cloud provider support the ability to take an existing running instance or a copy of an instance and export the instance into a virtual machine format?*

	• *If yes, what formats are supported?*
22.	***COMPUTE – SERVICE DISRUPTION:*** *Does the cloud provider offer mechanisms to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance at the host level?*
23.	***COMPUTE – INSTANCE RESTART:*** *Does the cloud provider offer mechanisms to automatically restart instances on a healthy host if the original physical host fails?*
24.	***COMPUTE – NOTIFICATIONS:*** *In the case of a compute resilient event, does the cloud provider have the ability to notify the user that such an event occurred, and is the user able to opt-in or opt-out of this communication via self-service means?*
25.	***COMPUTE – EVENT SCHEDULING:*** *Does the cloud provider offer the ability to schedule events for the user's instances, such as rebooting, stopping, starting, or retiring the instance?*
26.	***COMPUTE – BACKUP AND RESTORE MECHANISM:*** *Does the cloud provider offer an integrated backup and recovery mechanism?*
27.	***COMPUTE – SNAPSHOT MECHANISM:*** *Does the cloud provider offer a manual, on-demand snapshot mechanism?*
28.	***COMPUTE – METADATA:*** *Does the cloud provider offer an instance metadata service that allows users to set arbitrary key-value pairs for the instance?*
29.	***COMPUTE – METADATA CALL:*** *Does the cloud provider offer an instance metadata service that provides an application programming interface (API) that the instance can call to find out information about itself?*
30.	***COMPUTE – BIDDING MECHANISM:*** *Does the cloud provider offer a bidding mechanism to bid for lower-cost instances that can be immediately instantiated to host non-mission critical workloads?*
31.	***COMPUTE – SCHEDULING MECHANISM:*** *Does the cloud provider offer any way to schedule and reserve additional compute capacity on a recurring basis, i.e. daily, weekly, monthly schedule?*
32.	***COMPUTE – RESERVATION MECHANISM:*** *Does the cloud provider offer any way to reserve additional compute capacity for the future (i.e. 1yr, 2yrs, 3yrs, etc.)?*
33.	***COMPUTE – LINUX OPERATING SYSTEM:*** *Does the cloud provider support the last two long-term supported versions of at least one enterprise Linux distribution (such as Red Hat, SUSE) and one commonly used free Linux distribution (such as Ubuntu, CentOS, and Debian)?*
34.	***COMPUTE – WINDOWS OPERATING SYSTEM:*** *Does the cloud provider support the last two major Windows Server versions (Windows Server 2017 and Windows Server 2016)?*
35.	***COMPUTE – LICENSING PORTABILITY:*** *Does the cloud provider offer license portability and support?* • *If yes, please list software vendor, software names, editions, and its versions.*

36.	***COMPUTE – SERVICE LIMITS:*** *Does the cloud provider have any restrictions (i.e. service limits) in regards to the compute section above?* *Example:* *Maximum number of instances per account* *Maximum number of dedicated hosts per account* *Maximum number of reserved internet protocol (IP) addresses*

3.2 Networking

	Requirement
1.	***NETWORKING – VIRTUAL NETWORKS:*** *Does the cloud provider support the ability to create a logic, isolated virtual network that represents a company's own network in the cloud?*
2.	***NETWORKING – SAME REGION CONNECTIVITY:*** *Does the cloud provider support connecting two virtual networks within the same region to route traffic between them using private Internet protocol (IP) addresses?*
3.	***NETWORKING – DIFFERENT REGION CONNECTIVITY:*** *Does the cloud provider support connecting two virtual networks across different regions to route traffic between them using private Internet protocol (IP) addresses?*
4.	***NETWORKING – PRIVATE SUBNET:*** *Does the cloud provider offer the capability of creating fully isolated (private) virtual networks and subnets where instances can be provisioned without any public Internet protocol (IP) address or internet routing?*
5.	***NETWORKING – VIRTUAL NETWORK ADDRESS RANGE:*** *Does the cloud provider support Internet protocol (IP) address ranges specified in the request for comments (RFC) 1918 as well as publicly routable classless inter-domain routing (CIDR) blocks?*
6.	***NETWORKING – MULTIPLE PROTOCOLS:*** *Does the cloud provider support multiple protocols including transmission control protocol (TCP), user datagram protocol (UDP), and Internet control message protocol (ICMP)?*
7.	***NETWORKING – AUTO-ASSIGNMENT FOR IP ADDRESSES:*** *Does the cloud provider support the capability of automatically assigning public Internet protocol (IP) addresses to instances?*
8.	***NETWORKING – RESERVED STATIC IP ADDRESSES:*** *Does the cloud provider support Internet protocol (IP) addresses associated with a user account, not a particular instance? The IP address should remain associated with the account until released explicitly.*
9.	***NETWORKING – IPV6 SUPPORT:*** *Does the cloud provider support Internet protocol version 6 (IPv6) at either the gateway or instance level and expose this functionality to users?*
10.	***NETWORKING – MULTIPLE IP ADDRESSES PER NIC:*** *Does the cloud provider support the ability to assign a primary and a secondary Internet protocol (IP) address to a network interface card (NIC) that is attached to a given instance?*

11.	***NETWORKING – MULTIPLE NICS:*** *Does the cloud provider support the ability to assign multiple network interface cards (NICs) to a given instance?*
12.	***NETWORKING – NIC AND IP MOBILITY:*** *Does the cloud provider support the ability to move network interface cards (NICs) as well as Internet protocol (IP) addresses between instances?*
13.	***NETWORKING – SR-IOV SUPPORT:*** *Does the cloud provider support capabilities such as single root input/output virtualization (SR-IOV) for higher performance (i.e. packets per second - PPS), lower latency, and lower jitter?*
14.	***NETWORKING – INGRESS FILTERING:*** *Does the cloud provider support adding or removing rules applicable to inbound traffic (ingress) to instances?*
15.	***NETWORKING – EGRESS FILTERING:*** *Does the cloud provider support adding or removing rules applicable to outbound traffic (egress) originating from instances?*
16.	***NETWORKING – ACL:*** *Does the cloud provider offer access control lists (ACLs) to control inbound and outbound traffic to subnets?*
17.	***NETWORKING – FLOW LOG SUPPORT:*** *Does the cloud provider offer the capability of capturing network traffic flow logs?*
18.	***NETWORKING – NAT:*** *Does the cloud provider provide a network address translation (NAT) gateway managed service to enable instances in a private network to connect to the internet or other cloud services, but prevent the Internet from initiating a connection to those instances?*
19.	***NETWORKING – SOURCE/DESTINATION CHECK:*** *Does the cloud provider have the ability to disable source/destination check on network interface cards (NICs)?*
20.	***NETWORKING – VPN SUPPORT:*** *Does the cloud provider support virtual private network (VPN) connectivity between the cloud provider and the user's data centre?*
21.	***NETWORKING – VPN TUNNELS:*** *Does the cloud provider support multiple virtual private network (VPN) connections per virtual network?*
22.	***NETWORKING – IPSEC VPN SUPPORT:*** *Does the cloud provider allow users to access cloud services via either an Internet protocol security (IPsec) virtual private network (VPN) tunnel or secure sockets layer (SSL) virtual private network (VPN) tunnel over the public Internet?*
23.	***NETWORKING – BGP SUPPORT:*** *Does the cloud provider employ border gateway protocol (BGP) to improve failover across Internet protocol security (IPsec) virtual private network (VPN) tunnels?*
24.	***NETWORKING – PRIVATE DEDICATED CONNECTIVITY:*** *Does the cloud provider offer a direct, private connectivity service between the cloud provider's locations and a user's data centre, office, or colocation environment that allows for large and fast data transfers?*
25.	***NETWORKING – FRONT-END LOAD BALANCER:*** *Does the cloud provider offer a front-end (Internet-facing) load balancing service that takes requests from clients over the Internet and distributes these requests across instances that are registered with the load balancer?*

26.	***NETWORKING – BACK-END LOAD BALANCER:*** *Does the cloud provider offer a back-end (private) load balancing service that routes traffic to instances hosted in private subnets?*
27.	***NETWORKING – LAYER 7 LOAD BALANCER:*** *Does the cloud provider offer a layer 7 (hypertext transfer protocol - HTTP) load balancer service capable of load balancing network traffic across multiple instances?*
28.	***NETWORKING – LAYER 4 LOAD BALANCER:*** *Does the cloud provider offer a layer 4 (transmission control protocol - TCP) load balancer service capable of load balancing network traffic across multiple instances?*
29.	***NETWORKING – SESSION AFFINITY FOR LOAD BALANCERS:*** *Does the cloud provider offer a load balancing service that supports session affinity?*
30.	***NETWORKING – DNS-BASED LOAD BALANCING:*** *Does the cloud provider offer a load balancing service capable of load balancing traffic to instances hosted in multiple hosts that belong to a single domain?*
31.	***NETWORKING – LOAD BALANCER LOGS:*** *Does the cloud provider provide logs that capture detailed information about all requests sent to a load balancer?*
32.	***NETWORKING – DNS:*** *Does the cloud provider offer a highly available and scalable domain name system (DNS) service?*
33.	***NETWORKING – LATENCY-BASED DNS ROUTING:*** *Does the cloud provider offer a domain name system (DNS) service that supports latency-based routing (i.e. DNS service responds to DNS queries with the resources that provide the best latency)?*
34.	***NETWORKING – GEO-BASED DNS ROUTING:*** *Does the cloud provider offer a domain name system (DNS) service that supports geo-based routing (i.e. DNS service responds to DNS queries based on the geographic location of users)?*
35.	***NETWORKING – FAILOVER-BASED DNS ROUTING:*** *Does the cloud provider offer a domain name system (DNS) service that supports failover-based routing (i.e. DNS service routes DNS queries to the resource that is currently active, while a second resource waits and only becomes active in the event of a failure in the primary resource)?*
36.	***NETWORKING – DOMAIN REGISTRATION SERVICE:*** *Does the cloud provider offer domain name registration services (i.e. users can search for and register available domain names)?*
37.	***NETWORKING – DNS HEALTH CHECKS:*** *Does the cloud provider offer a domain name system (DNS) service that uses health checks to monitor the health and performance of resources?*
38.	***NETWORKING – DNS AND LOAD BALANCER INTEGRATION:***

	Does the cloud provider offer a domain name system (DNS) service that integrates with the cloud provider's load balancer?
39.	*NETWORKING – VISUAL EDITOR:* *Does the cloud provider offer a tool that allows users to build policies for traffic management?*
40.	*CONTENT DELIVERY NETWORK (CDN):* *Does the cloud provider offer a content delivery network (CDN) service to distribute content with low latency and high data transfer speeds?*
41.	*NETWORKING – CDN CACHE EXPIRATION:* *Does the cloud provider offer a content delivery network (CDN) service that allows to remove an object from edge caches before it expires, including features like invalidating objects and object versioning?*
42.	*NETWORKING – CDN EXTERNAL ORIGINS:* *Does the cloud provider offer a content delivery network (CDN) service that supports a custom origin, i.e., an hypertext transfer protocol (HTTP) server?*
43.	*NETWORKING – CDN OPTIMIZATION:* *Does the cloud provider offer a content delivery network (CDN) service with granular control for configuring multiple origin servers and caching properties for different uniform resource locators (URLs)?*
44.	*NETWORKING – CDN GEO-RESTRICTED:* *Does the cloud provider offer a content delivery network (CDN) service that supports geo restriction, i.e., preventing users in specific geographies from accessing content?*
45.	*NETWORKING – CDN TOKENS:* *Does the cloud provider offer a content delivery network (CDN) service that supports signed uniform resource locators (URLs) that would typically include additional information such as expiration date/time in order to give users more control over access to their content?*
46.	*NETWORKING – CDN CERTIFICATES:* *Does the cloud provider offer a content delivery network (CDN) service that supports custom secure sockets layer (SSL) certificates in order to deliver content securely over hypertext transfer protocol secure (HTTPS) from edge locations?*
47.	*NETWORKING – CDN MULTI-TIER CACHE:* *Does the cloud provider offer a content delivery network (CDN) service that employs a multi-tier cache approach with the use of regional edge caches in order to reduce latency?*
48.	*NETWORKING – CDN COMPRESSION:* *Does the cloud provider offer a content delivery network (CDN) service that supports file compression?*
49.	*NETWORKING – CDN ENCRYPTED UPLOADS:* *Does the cloud provider offer a content delivery network (CDN) that allows users to securely upload their sensitive data in a way that such information can only be viewed by certain components and services in user's origin infrastructure?*
50.	*NETWORKING – ENDPOINTS:* *Does the cloud provider's networking service offer users with endpoints capable of routing traffic through provider's internal network connectivity (i.e. private connectivity) in order to reduce communications costs and improve traffic security?*
51.	*NETWORKING – SERVICE LIMITS:* *Does the cloud provider have any restrictions (i.e. service limits) in regards to the networking section above?*

	Example: *Maximum number of virtual networks per account* *Maximum size of a virtual network* *Maximum number of subnets per account* *Maximum number of load balancers per account* *Maximum number of access control list (ACL) entries* *Maximum number of virtual private network (VPN) tunnels* *Maximum number of origins per distribution* *Maximum number of certificates per load balancer*

3.3 Storage

	Requirement
1.	***BLOCK STORAGE SERVICE:*** *Does the cloud provider offer block level storage volumes to use with compute instances?*
2.	***BLOCK STORAGE – IOPS:*** *Does the cloud provider offer the option of purchasing an explicit performance target or performance tier on block storage volumes, such as a certain number of input/output operations per second (IOPS) or megabytes per second (MB/S) of throughput?*
3.	***BLOCK STORAGE – SOLID STATE DRIVES:*** *Does the cloud provider support solid state drive (SSD) backed storage media that offers single digit millisecond latencies?* • *If yes, what is the maximum number of SSDs that can be attached per instance?*
4.	***BLOCK STORAGE – SCALING:*** *Does the cloud provider offer users the ability to increase the size of an existing block storage volume without having to provision a new volume and copy/move the data?*
5.	***BLOCK STORAGE – SNAPSHOTS:*** *Does the cloud provider have snapshot capability for its block storage service?*
6.	***BLOCK STORAGE – DATA ERADICATION:*** *Does the cloud provider support complete eradication of data such that data is no longer readable or accessible by unauthorized users and/or third parties?*
7.	***BLOCK STORAGE – ENCRYPTION AT-REST:*** *Does the cloud provider offer server-side encryption of data at-rest for data stored on volumes and its snapshots?* • *If yes, what is the cryptographic algorithm employed?*
8.	***OBJECT STORAGE SERVICE:*** *Does the cloud provider offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web?*
9.	***OBJECT STORAGE – INFREQUENT ACCESS:*** *Does the cloud provider offer a lower-cost storage service tier aimed at storing less-frequently accessed objects and files?*

10.	***OBJECT STORAGE – LOWER DURABILITY:*** *Does the cloud provider offer a reduced redundancy tier where a user can store non-critical, easy-reproducible objects at a lower price?*
11.	***OBJECT STORAGE – LESS FREQUENT ACCESS:*** *Does the cloud provider offer a tier for less-frequently accessed data, but that still requires rapid access?*
12.	***OBJECT STORAGE – OBJECT TIERING:*** *Does the cloud provider offer object storage tiering capability, i.e. the ability to recommend transitioning an object between object storage classes or tiers based on its frequency of access?*
13.	***OBJECT STORAGE – LIFECYCLE MANAGEMENT:*** *Does the cloud provider support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation to deletion?*
14.	***OBJECT STORAGE – POLICY-DRIVEN MANAGEMENT:*** *Does the cloud provider offer the ability to create and use policies to manage stored data, its lifecycle, and its tiering settings?*
15.	***OBJECT STORAGE – LOCATION AND TIME-BASED POLICIES:*** *Does the cloud provider offer users the capability to create policies that can restrict access to the data based on user's location and time of request?*
16.	***OBJECT STORAGE – WEBSITE HOSTING:*** *Does the cloud provider support hosting static websites out of its object storage service?*
17.	***OBJECT STORAGE – ENCRYPTION AT-REST:*** *Does the cloud provider support server-side encryption (SSE) of data at-rest, with the cloud provider managing the encryption keys?* • *If yes, what is the cryptographic algorithm employed?*
18.	***OBJECT STORAGE – ENCRYPTION WITH USER KEYS:*** *Does the cloud provider offer server-side encryption (SSE) capabilities using customer provided cryptographic keys?*
19.	***OBJECT STORAGE – KEY MANAGED SERVICE:*** *Does the cloud provider support server-side encryption (SSE) using a key management service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly?*
20.	***OBJECT STORAGE – CLIENT-SIDE MASTER KEY:*** *Does the cloud provider offer users the option of retaining control of the encryption keys and complete the encryption/decryption of objects client-side?*
21.	***OBJECT STORAGE – STRONG CONSISTENCY:*** *Does the cloud provider support read-after-write consistency for PUT operations for new objects?*
22.	***OBJECT STORAGE – DATA LOCALITY:*** *Does the cloud provider offer a strong regional isolation, so that objects stored in a region never leave the region unless user explicitly transfers them to another region?*
23.	***OBJECT STORAGE – REPLICATION:*** *Does the cloud provider offer a cross-regional replication feature that will automatically replicate objects across user-selected regions?*
24.	***OBJECT STORAGE – VERSIONING:***

	Does the cloud provider support versioning, i.e. the ability to store and maintain multiple versions of an object?
25.	***OBJECT STORAGE – UNDELETE MARKER:*** *Does the cloud provider allow a user to mark an item as undeletable?*
26.	***OBJECT STORAGE – MFA DELETE:*** *Does the cloud provider support multi-factor authentication (MFA) for delete operations as an additional security option?*
27.	***OBJECT STORAGE – MULTIPART UPLOAD:*** *Does the cloud provider allow uploading an object as a set of parts, where each part is a contiguous portion of the object's data and these objects parts can be uploaded independently and in any order?*
28.	***OBJECT STORAGE – TAGS:*** *Does the cloud provider offer the ability to create and associate mutable, dynamic tags at the object level?*
29.	***OBJECT STORAGE – NOTIFICATIONS:*** *Does the cloud provider offer the ability to send notifications when certain events happen at the object level (i.e. addition/deletion operations)?*
30.	***OBJECT STORAGE – LOGS:*** *Does the cloud provider offer the capability of generating audit logs that include details about a single access request, such as the requester, the request time, the request action, the response status, and the error code?*
31.	***OBJECT STORAGE – INVENTORY FOR OBJECTS:*** *Does the cloud provider offer object inventory capability to give users the ability to quickly visualize objects and their status, allowing users to quickly spot objects with public access?*
32.	***OBJECT STORAGE – INVENTORY FOR METADATA:*** *Does the cloud provider offer object inventory capability to give users the ability to quickly visualize objects' metadata?*
33.	***OBJECT STORAGE – UPLOADS OPTIMIZATION:*** *Does the cloud provider have the ability to route data from edge locations to the storage service using an optimized network path?*
34.	***OBJECT STORAGE – QUERY CAPABILITY:*** *Does the cloud provider offer users the ability to query its object storage service by using structured query language (SQL) statements?*
35.	***OBJECT STORAGE – SUBSET RETRIEVAL:*** *Does the cloud provider offer users the ability to retrieve only a subset of data from an object by using simple structured query language (SQL) expressions?*
36.	***FILE STORAGE SERVICE:*** *Does the cloud provider offer a simple and scalable file storage service to use with compute instances in the cloud?*
37.	***FILE STORAGE – REDUNDANCY:***

	Does the cloud provider redundantly stores the file system objects (i.e. directory, file, and link) across multiple data centres or facilities to achieve higher levels of availability and durability?
38.	***FILE STORAGE – DATA ERADICATION:*** *Does the cloud provider support complete eradication of file storage data such that it is no longer readable or accessible by unauthorized users or third parties?*
39.	***FILE STORAGE – HIGH AVAILABILITY:*** *Does the cloud provider's managed file system provide a high degree of high availability?*
40.	***FILE STORAGE – NFS:*** *Does the cloud provider support the network file system (NFS) protocol?*
41.	***FILE STORAGE – SMB:*** *Does the cloud provider support the server message block (SMB) protocol?*
42.	***FILE STORAGE – ENCRYPTION AT-REST:*** *Does the cloud provider's file storage service support encryption at-rest?*
43.	***FILE STORAGE – ENCRYPTION IN-TRANSIT:*** *Does the cloud provider's file storage service support encryption of data while in-transit?*
44.	***FILE STORAGE – DATA MIGRATION TOOL:*** *Does the cloud provider offer any data migration tool to allow users to move data from on-premises systems to the cloud-based file system?*
45.	***ARCHIVE STORAGE SERVICE:*** *Does the cloud provider offer a very low-cost storage service aimed at archiving less-frequently accessed and almost immutable objects and files?*
46.	***ARCHIVE STORAGE – FAULT TOLERANCE:*** *Does the cloud provider architecture provide fault tolerance for its archival storage service?*
47.	***ARCHIVE STORAGE – IMMUTABILITY:*** *Does the cloud provider support immutability of the archived objects and files?*
48.	***ARCHIVE STORAGE – WORM:*** *Does the cloud provider offer write once read many (WORM) capability?*
49.	***ARCHIVE STORAGE – SUBSET RETRIEVAL:*** *Does the cloud provider offer users the ability to retrieve only a subset of data from an archived object by using simple structured query language (SQL) expressions?*
50.	***ARCHIVE STORAGE – SPEED RETRIEVAL:*** *Does the cloud provider offer users multiple options of data retrieval with different costs and retrieval times?*
51.	***ARCHIVE STORAGE – ENCRYPTION AT-REST:*** *Does the cloud provider's archive storage service support encryption at-rest?*
52.	***STORAGE – SERVICE LIMITS:*** *Does the cloud provider have any restrictions (i.e. service limits) in regards to the storage section above?* *Example:* *Maximum volume size*

	Maximum number of drives attached to an instance *Maximum input/output operations per second (IOPS)* *Maximum object size* *Maximum number of objects per storage account* *Maximum number of snapshots*

4. Administration

	Requirement
1.	***ADMINISTRATION – USERS AND GROUPS:*** *Does the cloud provider offer a service to create and manage users and groups of users of its infrastructure and its resources?*
2.	***ADMINISTRATION – PASSWORD RESET:*** *Does the cloud provider allow users to reset their own password in a self-service manner?*
3.	***ADMINISTRATION – PERMISSIONS:*** *Does the cloud provider offer the ability to add permissions to users and groups at the resource-level?*
4.	***ADMINISTRATION – TEMPORARY PERMISSIONS:*** *Does the cloud provider offer the ability to create permissions that are valid for a specific interval of time?*
5.	***ADMINISTRATION – TEMPORARY CREDENTIALS:*** *Does the cloud provider offer users the ability to create and provide temporary security credentials to trusted users configured to last for anywhere from a few minutes to several hours?*
6.	***ADMINISTRATION – ACCESS CONTROL:*** *Does the cloud provider offer fine-grained access controls to its infrastructure resources?* • *If yes, what conditions can be used by these controls (i.e. time of the day, originating IP address, etc.)?*
7.	***ADMINISTRATION – BUILT-IN POLICIES:*** *Does the cloud provider infrastructure contains built-in access control policies that can be attached to users and groups?*
8.	***ADMINISTRATION – CUSTOM POLICIES:*** *Does the cloud provider infrastructure allows the creation and customization of access control policies that can be attached to users and groups?*
9.	***ADMINISTRATION – POLICY SIMULATOR:*** *Does the cloud provider offer a mechanism to test the effects of access control policies before committing such policies into production?*
10.	***ADMINISTRATION – CLOUD MFA:*** *Does the cloud provider support the use of multi-factor authentication (MFA) as an additional layer of access control and authentication to its infrastructure?*
11.	***ADMINISTRATION – SERVICE LIMITS:*** *Does the cloud provider have any restrictions (i.e. service limits) in regards to the administration section above?* *Example:*

	Maximum number of users *Maximum number of groups* *Maximum number of managed policies*

5. Security

	Requirement
1.	***SECURITY – BACKGROUND CHECKS:*** *Are all of the cloud provider's personnel who have access to service infrastructure (whether physical or non-physical) subject to background checks?*
2.	***SECURITY – PHYSICAL ACCESS:*** *Does the cloud provider restrict personnel from accessing service infrastructure unless there is a specific trouble ticket, change request, or similar formal authorization?*
3.	***SECURITY – ACCESS LOGS:*** *Does the cloud provider log personnel access over its infrastructure, where such access is always logged and logs are retained for a minimum of 90 days?*
4.	***SECURITY – HOST LOGINS:*** *Does the cloud provider restrict provider personnel from logging into compute hosts, instead automating all tasks carried out on compute hosts where the contents of these automated jobs are logged, with the logs retained for a minimum of 90 days?*
5.	***SECURITY – CRYPTOGRAPHIC KEYS:*** *Does the cloud provider offer a service to create and control the cryptographic keys used to encrypt user data?*
6.	***SECURITY – ACCESS KEY MANAGEMENT:*** *Does the cloud provider offer the ability to identify when an access key was last used, rotate old keys, and remove inactive users?*
7.	***SECURITY – CUSTOMER PROVIDED KEYS:*** *Does the cloud provider allow users to import keys from their own key management infrastructure to the cloud service provider's key management service?*
8.	***SECURITY – CRYPTOGRAPHIC KEYS SERVICE INTEGRATION:*** *Does the cloud provider's key management service integrate with other cloud services to provide data at-rest encryption capability?*
9.	***SECURITY – HSM:*** *Does the cloud provider offer dedicated hardware security modules (HSM), i.e. hardware appliances that provides secure key storage and cryptographic operations within a tamper-resistant hardware module?*
10.	***SECURITY – CRYPTOGRAPHIC KEYS DURABILITY:*** *Does the cloud provider support durability of keys, including storing multiple copies so that keys are available when needed?*
11.	***SECURITY – SSO:*** *Does the cloud provider offer a managed single sign-on (SSO) service that allows users to centrally manage access to multiple accounts and business applications?*
12.	***SECURITY – CERTIFICATES:***

	Does the cloud provider offer a managed service to provision, manage, and deploy secure sockets layer (SSL) / transport layer security (TLS) certificates?
13.	*SECURITY – CERTIFICATES RENEWAL:* *Does the cloud provider's certificate management service facilitate renewal of certificates?*
14.	*SECURITY – WILDCARD CERTIFICATES:* *Does the cloud provider's certificate management service support use of wildcard certificates?*
15.	*SECURITY – CERTIFICATE AUTHORITY:* *Does the cloud provider's certificate management service also acts as a certificate authority (CA)?*
16.	*SECURITY – ACTIVE DIRECTORY:* *Does the cloud provider offer a managed Microsoft active directory (AD) service in the cloud?*
17.	*SECURITY – ON-PREM ACTIVE DIRECTORY:* *Does the cloud provider's managed Microsoft active directory service (AD) support integration with on-premises Microsoft active directory (AD)?*
18.	*SECURITY – LDAP:* *Does the cloud provider's managed Microsoft active directory (AD) service support the lightweight directory access protocol (LDAP)?*
19.	*SECURITY – ACTIVE DIRECTORY:* *Does the cloud provider's managed Microsoft active directory (AD) service support security assertion markup language (SAML)?*
20.	*SECURITY – CREDENTIALS MANAGEMENT:* *Does the cloud provider offer a managed service that helps users easily rotate, manage, and retrieve credentials such as application programming interface (API) keys, database credentials, and other secrets?*
21.	*SECURITY – WAF:* *Does the cloud provider offer a web application firewall (WAF) that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources?*
22.	*SECURITY – DDOS:* *Does the cloud provider offer a service to protect from common, most frequently occurring network and transport layer distributed denial of service (DDoS) attacks, along with the ability to write customized rules to mitigate sophisticated application layer attacks?*
23.	*SECURITY – SECURITY RECOMMENDATIONS:* *Does the cloud provider offer a service to automatically assess potential vulnerabilities in applications and resources?*
24.	*SECURITY – THREAT DETECTION:* *Does the cloud provider offer a managed threat detection service?*
25.	*SECURITY – SERVICE LIMITS:* *Does the cloud provider have any restrictions (i.e. service limits) in regards to the security section above?* *Example:* *Maximum number of customer master keys* *Maximum number of hardware security modules (HSMs)*

6. Compliance

The list below has been provided for illustrative purposes only and should not be considered exhaustive of the certifications and standards that could apply to Cloud Services.

Please indicate which set of international and industry-specific compliance standards the cloud provider has met:

Certifications / Attestations	*Laws, Regulations, and Privacy*	*Alignments / Frameworks*
☐ *C5 [Germany]*	☐ *EU Data Protection Directive*	☐ *CDSA*
☐ *CISPE Data Protection Code of Conduct*	☐ *EU Model Clauses*	
☐ *CNDCP (Climate Neutral Data Centre Pact)*		
☐ *DIACAP*	☐ *FERPA*	☐ *CIS*
☐ *DoD SRG Levels 2 & 4*	☐ *GDPR*	☐ *Criminal Justice Info. Service (CJIS)*
☐ *FedRAMP*	☐ *GLBA*	☐ *CSA*
☐ *FIPS 140-2*	☐ *HIPAA*	☐ *EU-US Privacy Shield*
☐ *HDS (France, Healthcare)*	☐ *HITECH*	☐ *EU Safe Harbor*
☐ *ISO 9001*	☐ *IRS 1075*	☐ *FISC*
☐ *ISO 27001*	☐ *ITAR*	☐ *FISMA*
☐ *ISO 27017*	☐ *PDPA – 2010 [Malaysia]*	☐ *G-Cloud [UK]*
☐ *ISO 27018*	☐ *PDPA – 2012 [Singapore]*	☐ *GxP (FDA CFR 21 Part 11)*
☐ *IRAP [Australia]*	☐ *PIPEDA [Canada]*	☐ *ICREA*
☐ *MTCS Tier 3 [Singapore]*	☐ *Privacy Act [Australia]*	☐ *IT Grundschutz [Germany]*
☐ *PCI DSS Level 1*	☐ *Privacy Act [New Zealand]*	☐ *MARS – E*
☐ *SEC Rule 17-a-4(f)*	☐ *Spanish DPA Authorization*	☐ *MITA 3.0*
☐ *SOC1 / ISAE 3402*	☐ *U.K. DPA - 1988*	☐ *MPAA*
☐ *SOC2 / SOC3*	☐ *VPAT/Section 508*	☐ *NIST*
☐ *SWIPO IaaS Code*		
		☐ *Uptime Institute Tiers*
		☐ *UK Cloud Security Principles*

Leveraging the above compliance reports allows public sector organizations to evaluate unique offerings against accepted security, compliance and operational standard. Such reports can display that the CISP, through their compliance with them, meets the below data centre operation controls that are required of the public cloud service provider. Requiring compliance with such reports helps public sector entities have assurance that the below controls are place.

- ***Scrutinized access:*** *CISP should restrict physical access to those people who need to be at a location for a justified business reason. If access is granted, it should be revoked as soon as the necessary work is completed.*
- ***Entry controlled and monitored:*** *Entering the Perimeter Data Centre Layer should be a controlled process. CISP should staff entry gates with security officers and employ supervisors who monitor officers and visitors via security cameras. When approved individuals are on site, they should be given a badge that requires multi-factor authentication and limits access to pre-approved areas.*
- ***CISP data centre workers:*** *CISP employees who routinely need access to a data centre should be given permissions to relevant areas of the facility based on job function, with access regularly scrutinized. Staff lists should be routinely reviewed by an area access manager to ensure each employee's authorization is still necessary. If an employee doesn't have an ongoing business need to be at a data centre, they should be required to go through the visitor process.*
- ***Monitoring for unauthorized entry:*** *CISPs should continuously monitor for unauthorized entry on data centre property, using video surveillance, intrusion detection, and access log monitoring systems. Entrances should be secured with devices that sound alarms if a door is forced or held open.*
- ***CISP Security Operations Centres monitors global security:*** *CISP Security Operations Centres should be located around the world and responsible for monitoring, triaging, and executing security programs for CISP data centres. They should oversee physical access management and intrusion detection response while also providing global, 24/7 support to the on-site data centre security teams; providing continuous monitoring activities such as tracking access activities, revoking access permissions, and being available to respond to and analyse a potential security incident.*
- ***Layer-by-layer access review:*** *Access to the Infrastructure Layer should be restricted based on business need. By implementing a layer-by-layer access review, the right to enter every layer is not granted by default. Access to any particular layer should only be granted if there is a specific need to access that specific layer.*
- ***Maintaining equipment is a part of regular operations:*** *CISP teams should run diagnostics on machines, networks, and backup equipment to ensure they're in working order now, and in an emergency. Routine maintenance checks on data centre equipment and utilities should be part of regular CISP data centre operations.*
- ***Emergency-ready backup equipment:*** *Water, power, telecommunications, and internet connectivity should be designed with redundancy, so the CISP can maintain continuous operations in an emergency. Electrical power systems should be designed to be fully redundant so that in the event of a disruption, uninterruptible power supply units can be engaged for certain functions, while generators can provide backup power for the entire facility. People and systems should monitor and control the temperature and humidity to prevent overheating, further reducing possible service outages.*
- ***Technology and people work together for added security:*** *There should be mandatory procedures to obtain authorization to enter the Data Layer. This includes review and approval of a person's access application by authorized individuals. Meanwhile, threat and electronic intrusion detection systems should monitor and automatically trigger alerts of identified threats or suspicious activity. For example, if a door is held or forced open an alarm is triggered. CISP should deploy security cameras and retain footage in alignment with legal and compliance requirements.*
- ***Preventing physical and technological intrusion:*** *Access points to server rooms should be fortified with electronic control devices that require multi-factor authorization. CISP should also be prepared to prevent technological intrusion. CISP servers should be able to warn employees of any attempts to remove data. In the unlikely event of a breach, the server should be automatically disabled.*
- ***Servers and media receive exacting attention:*** *Media storage devices used to store customer data should be classified by the CISP as Critical and treated accordingly, as high impact, throughout their life-cycle. The CISP should have exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, the CISP will decommission media using techniques detailed in NIST 800-88. Media that stored customer data is not removed from CISP control until it has been securely decommissioned.*

- ***Third-party auditors verify CISP procedures and systems:*** *CISP should be audited by external auditors to inspect data centres, performing a deep dive to confirm the CISP is following established rules needed to obtain its security certifications. Depending on the compliance program and its requirements, external auditors may interview CISP employees about how they handle and dispose of media. Auditors may also watch security camera feeds and observe entrances and hallways throughout a data centre. And they may examine equipment such as CISP electronic access control devices and security cameras.*

- ***Prepared for the unexpected:*** *CISP should proactively prepare for potential environmental threats, like natural disasters and fire. Installing automatic sensors and responsive equipment are two ways the CISP will safeguard data centres. Water-detecting devices should be installed to alert employees to problems as automatic pumps work to remove liquid and prevent damage. Similarly, automatic fire detection and suppression equipment reduce risk and can notify CISP employees and firefighters of a problem.*

- ***High Availability through Multiple Availability Zones:*** *CISP should provide multiple Availability Zones for greater fault tolerance. Each Availability Zone should consist of one or more data centre, be physically separated from one another, and have redundant power and networking. Availability Zones should be connected to each other with fast, private fiber-optic networking, in order to architect applications that automatically fail-over between Availability Zones without interruption.*

- ***Simulating disruptions & measuring our response****: The CISP should have a Business Continuity Plan as an operations process guide outlining how to avoid and lessen disruptions due to natural disasters, with detailed steps to take before, during, and after an event. To mitigate and prepare for the unexpected, CISP should test the Business Continuity Plan regularly with drills that simulate different scenarios. CISP should document how its people and processes perform, then debrief on lessons learned and any corrective actions that may be needed to improve response rate. CISP staff should be trained and ready to rebound from disruptions quickly, with a methodical recovery process to minimize further downtime due to errors.*

- ***Help meet efficiency targets:*** *In addition to addressing environmental risks, CISP should also incorporate sustainability considerations into data centre design. CISP should provide details of its commitment to use renewable energy for its data centres, and provide information as to how its customers can reduce carbon emissions versus their own data centres.*

- ***Site Selection****: Prior to choosing a location, the CISP should perform initial environmental and geographic assessments. Data centre locations should be carefully selected to mitigate environmental risks, such as flooding, extreme weather, and seismic activity. CISP Availability Zones should be built to be independent and physically separated from one another.*

- ***Redundancy:*** *Data centres should be designed to anticipate and tolerate failure while maintaining service levels. In case of failure, automated processes should move traffic away from the affected area. Core applications should be deployed to an N+1 standard, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.*

- ***Availability:*** *CISP should identify critical system components required to maintain the availability of its system, and recover service in the event of outage. Critical system components should be backed up across multiple, isolated locations. Each location or Availability Zone should be engineered to operate independently with high reliability. Availability Zones should be connected to enable applications to automatically fail-over between Availability Zones without interruption. Highly resilient systems, and therefore service availability, should be a function of the system design. Data centre design with Availability Zones and data replication should enable CISP customers to achieve extremely short recovery time and recovery point objectives, as well as the highest levels of service availability.*

- ***Capacity Planning****: CISP should continuously monitor service usage to deploy infrastructure to support availability commitments and requirements. CISP should maintain a capacity planning model that assesses CISP infrastructure usage and demands at least monthly. This model should support planning of future demands and include considerations such as information processing, telecommunications, and audit log storage.*

BUSINESS CONTINUITY and DISASTER RECOVERY

- ***Business Continuity Plan:*** *The CISP Business Continuity Plan should outline measures to avoid and lessen environmental disruptions. It should include operational details about steps to take before, during, and after an event. The Business Continuity Plan should be supported by testing that includes simulations of different scenarios. During and after testing, the CISP should document people and process performance, corrective actions, and lessons learned with the aim of continuous improvement.*

- ***Pandemic Response:*** *The CISP should incorporates pandemic response policies and procedures into its disaster recovery planning to prepare to respond rapidly to infectious disease outbreak threats. Mitigation strategies include alternative staffing models to transfer critical processes to out-of-region resources, and activation of a crisis management plan to support critical business operations. Pandemic plans should reference international health agencies and regulations, including points of contact for international agencies.*

MONITORING and LOGGING

- ***Data Centre Access Review:*** *Access to data centres should be regularly reviewed. Access should be automatically revoked when an employee's record is terminated in the CISP's HR system. In addition, when an employee or contractor's access expires in accordance with the approved request duration, his or her access should be revoked, even if he or she continues to be an employee of the CISP.*

- ***Data Centre Access Logs****: Physical access to CISP data centres should be logged, monitored, and retained. CISP should correlate information gained from logical and physical monitoring systems to enhance security on an as-needed basis.*

- ***Data Centre Access Monitoring:*** *CISP should monitor data centres using global Security Operations Centres - responsible for monitoring, triaging, and executing security programs. They should provide 24/7 global support by managing and monitoring data centre access activities, equipping local teams and other support teams to respond to security incidents by triaging, consulting, analysing, and dispatching responses.*

SURVEILLANCE and DETECTION

- ***CCTV:*** *Physical access points to server rooms should be recorded by Closed Circuit Television Camera (CCTV). Images should be retained according to legal and compliance requirements.*

- ***Data Centre Entry Points:*** *Physical access should be controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff should utilize multi-factor authentication mechanisms to access data centres. Entrances to server rooms should be secured with devices that sound alarms to initiate an incident response if the door is forced or held open.*

- ***Intrusion Detection:*** *Electronic intrusion detection systems should be installed within the data layer to monitor, detect, and automatically alert appropriate personnel of security incidents. Ingress and egress points to server rooms should be secured with devices that require each individual to provide multi-factor authentication before granting entry or exit. These devices will sound alarms if the door is forced open without authentication or held open. Door alarming devices should also be configured to detect instances where an individual exits or enters a data layer without providing multi-factor authentication. Alarms should be immediately dispatched to 24/7 CISP Security Operations Centres for immediate logging, analysis, and response.*

DEVICE MANAGEMENT

- ***Asset Management:*** *CISP assets should be centrally managed through an inventory management system that stores and tracks owner, location, status, maintenance, and descriptive information for CISP-owned assets. Following procurement, assets should be scanned and tracked, and assets undergoing maintenance checked and monitored for ownership, status, and resolution.*

- ***Media Destruction:*** *Media storage devices used to store customer data should classified by the CISP as Critical and treated accordingly, as high impact, throughout their life-cycles. CISP should have exacting standards on how to install, service, and eventually destroy the devices when they are no longer useful. When a storage device has reached the end of its useful life, CISP should decommission media using techniques detailed in NIST 800-88. Media that stored customer data should be not removed from CISP control until it has been securely decommissioned.*

OPERATIONAL SUPPORT SYSTEMS

- ***Power:*** *CISP data centre electrical power systems should be designed to be fully redundant and maintainable without impact to operations, 24 hours a day. CISP should ensure that data centres are equipped with back-up power supply to ensure power is available to maintain operations in the event of an electrical failure for critical and essential loads in the facility.*

- ***Climate and Temperature:*** *CISP data centres should use mechanisms to control climate and maintain an appropriate operating temperature for servers and other hardware to prevent overheating and reduce the possibility of service outages. Personnel and systems should monitor and control temperature and humidity at appropriate levels.*

- ***Fire Detection and Suppression****: CISP data centres should be equipped with automatic fire detection and suppression equipment. Fire detection systems should utilize smoke detection sensors within networking, mechanical, and infrastructure spaces. These areas should also be protected by suppression systems.*

- ***Leakage Detection:*** *In order to detect the presence of water leaks, CISP should equip data centres with functionality to detect the presence of water. If water is detected, mechanisms should be in place to remove water in order to prevent any additional water damage.*

INFRASTRUCTURE MAINTENANCE

- ***Equipment Maintenance****: CISP should monitor and perform preventative maintenance of electrical and mechanical equipment to maintain the continued operability of systems within CISP data centres. Equipment maintenance procedures should be carried out by qualified persons and completed according to a documented maintenance schedule.*

- ***Environment Management:*** *CISP should monitor electrical and mechanical systems and equipment to enable immediate identification of issues. This should be carried out by utilizing continuous audit tools and information provided through CISP Building Management and Electrical Monitoring Systems. Preventative maintenance should be performed to maintain the continued operability of equipment.*

GOVERNANCE & RISK

- ***Ongoing Data Centre Risk Management:*** *The CISP Security Operations Centre should perform regular threat and vulnerability reviews of data centres. Ongoing assessment and mitigation of potential vulnerabilities should be performed through data centre risk assessment activities. This assessment should be performed in addition to the enterprise-level risk assessment process used to identify and manage risks presented to the business as a whole. This process should also take regional regulatory and environmental risks into consideration.*

- ***Third-Party Security Attestation:*** *Third-party testing of CISP data centres, as documented in its third-party reports, should ensure that the CISP has appropriately implemented security measures aligned to established rules needed to obtain security certifications. Depending on the compliance program and its requirements, external auditors may perform testing of media disposal, review security camera footage, observe entrances and hallways throughout a data centre, test electronic access control devices, and examine data centre equipment.*

7. Migrations

	Requirement
1.	***MIGRATIONS SERVICE:*** *How many different data migration services do the cloud provider offer?*
2.	***MIGRATIONS – CENTRALIZED MONITORING:*** *Does the cloud provider offer organizations a centralized (i.e. single pane of glass) service, where they can track and monitor the status of their server and application migrations?*
3.	***MIGRATIONS – DASHBOARD:*** *Does the cloud provider's migration tool offer a dashboard to quickly visualize migration status, related metrics, and migration history?*
4.	***MIGRATIONS – CLOUD PROVIDER TOOLS:*** *Does the cloud provider's migration tool offer integration with other migration tools from the cloud provider that can perform server and application migrations?*
5.	***MIGRATIONS – THIRD-PARTY TOOLS:*** *Does the cloud provider's migration tool allow to incorporate third-party migration tools?*

	• *If yes, what are the supported third-party migration tools?*
6.	***MIGRATIONS – MULTI-REGION MIGRATIONS:*** *Does the cloud provider's migration tool offer tracking and monitoring ability for server and application migrations happening in different regions?*
7.	***MIGRATIONS – SERVER MIGRATION:*** *Does the cloud provider's migration tool offer a way to migrate on-premises virtualized servers to the cloud?* • *If yes, what virtualized environments are currently supported?*
8.	***MIGRATIONS – SERVER DISCOVERY:*** *Does the cloud provider's migration tool have discovery capability to automatically find on-premises virtual servers to be migrated to the cloud?*
9.	***MIGRATIONS – SERVER PERFORMANCE DATA:*** *Does the cloud provider's migration tool have the capability to collect and display server and/or virtual machine performance like central processing unit (CPU) and random access memory (RAM) utilization?*
10.	***MIGRATIONS – DISCOVERY DATABASE:*** *Does the cloud provider's migration tool have the ability to store all collected data in a centralized database?* • *If yes, do organizations have the ability to export these data? To what formats?*
11.	***MIGRATIONS – ENCRYPTION AT-REST:*** *Does the cloud provider encrypt at-rest all information collected and stored in the discovery database?*
12.	***MIGRATIONS – INCREMENTAL SERVER REPLICATION:*** *Does the cloud provider's migration tool offer automated, live incremental server replication during the server or virtual machine migration as a way to support all changes made to the server or virtual machine are included in the final migrated image?* • *If yes, for how long can this service run?*
13.	***MIGRATIONS – VMWARE:*** *Does the cloud provider's migration tool support VMWare virtual machine migrations from on-premises to the cloud?*
14.	***MIGRATIONS – HYPER-V:*** *Does the cloud provider's migration tool support Hyper-V virtual machine migrations from on-premises to the cloud?*
15.	***MIGRATIONS – APPLICATION DISCOVERY:*** *Does the cloud provider's migration tool have the ability to discover and group applications before they get migrated?*
16.	***MIGRATIONS – DEPENDENCY MAPPING:*** *Does the cloud provider's migration tool have the ability to discover dependencies between servers and applications before they get migrated?*
17.	***MIGRATIONS – DATABASE MIGRATION:*** *Does the cloud provider's migration tool have the capability of migrating on-premises databases to the cloud?*
18.	***MIGRATIONS – DATABASE MIGRATION DOWNTIME:*** *Does the cloud provider's migration tool have the capability of performing a database migration to the cloud with minimum downtime, i.e., the source database should remain fully operational during the migration process?*
19.	***MIGRATIONS – SOURCE DATABASE:*** *Does the cloud provider's migration tool support migrating different database sources like Oracle, SQL Server, etc…?* • *If yes, please list all supported source databases that can be migrated to the cloud.*

20.	***MIGRATIONS – HETEROGENEOUS MIGRATIONS:*** *Does the cloud provider's migration tool have the ability to perform heterogeneous database migrations, i.e., from one source database to a different target database like from Oracle to SQL Server?* • *If yes, please list all possible heterogeneous database migration combinations.*
21.	***MIGRATIONS – PETABYTE-SCALE DATA MIGRATION:*** *Does the cloud provider offer a petabyte-scale data transport solution that uses secure appliances to transfer large amounts of data into and out of the cloud?*
22.	***MIGRATIONS – EXABYTE-SCALE DATA MIGRATION:*** *Does the cloud provider offer an Exabyte-scale data transport solution to move extremely large amounts of data to the cloud?*
23.	***MIGRATIONS – ENTERPRISE BACKUPS:*** *Does the cloud provider offer a service to seamlessly integrate a customer's data centre with cloud storage services that will allow to transfer and store data into the cloud provider's storage service?*
24.	***MIGRATIONS – ENTERPRISE BACKUPS – OBJECT STORAGE:*** *Does the cloud provider's enterprise backup service offer integration with provider's cloud object storage service?*
25.	***MIGRATIONS – ENTERPRISE BACKUPS – FILE ACCESS:*** *Does the cloud provider's enterprise backup service allow users to store and retrieve objects using file protocols like the network file system (NFS) protocol?*
26.	***MIGRATIONS – ENTERPRISE BACKUPS – BLOCK ACCESS:*** *Does the cloud provider's enterprise backup service allow users to store and retrieve objects using block protocols like the Internet small computer systems interface (iSCSI) protocol?*
27.	***MIGRATIONS – ENTERPRISE BACKUPS – TAPE ACCESS:*** *Does the cloud provider's enterprise backup service allow users to backup their data through a virtual tape library and store these tape backups in the provider's cloud?*
28.	***MIGRATIONS – ENTERPRISE BACKUPS - ENCRYPTION:*** *Does the cloud provider's enterprise backup service offer encryption of data at-rest and in-transit?*
29.	***MIGRATIONS – ENTERPRISE BACKUPS – THIRD-PARTY SOFTWARE INTEGRATION:*** *Does the cloud provider's enterprise backup service integrate with commonly used third-party backup software?*
30.	***MIGRATIONS – SERVICE LIMITS:*** *Does the cloud provider have any restrictions (i.e. service limits) in regards to the migrations section above?* *Example:* *Maximum number of concurrent virtual machine migrations* *Maximum orderable number of data transport solutions*

8. Billing

	Requirement
1.	***BILLING – TRACKING AND REPORTING:*** *Does the cloud provider offer a tracking and reporting billing service to help users manage and monitor their usage of cloud offerings?*

2.	***BILLING – ALARMS AND NOTIFICATIONS:*** *Does the cloud provider offer users a mechanism to set up alarms with notifications to alert users when their spending has crossed a specific threshold?*
3.	***BILLING – COST MANAGEMENT:*** *Does the cloud provider offer a mechanism to build and display graphics that summarize costs and spending?*
4.	***BILLING – BUDGETS:*** *Does the cloud provider offer a mechanism to display and manage budgets and forecast estimated costs?*
5.	***BILLING – CONSOLIDATED VIEW:*** *Does the cloud provider offer a mechanism to consolidate billing from multiple accounts under a single, primary paying account?*
6.	***BILLING – SERVICE LIMITS:*** *Does the cloud provider have any restrictions (i.e. service limits) in regards to the billing section above?* *Example:* *Maximum number of accounts that can be grouped together* *Maximum number of alarms that can be created* *Maximum number of budgets that can be managed*

9. Management

	Requirement
1.	***MANAGEMENT – MONITORING SERVICE:*** *Does the cloud provider offer a monitoring service for managing cloud resources and applications that collects, monitors, and reports using pre-defined metrics?*
2.	***MANAGEMENT – ALARMS:*** *Does the cloud provider's monitoring service allow users to set up alarms?*
3.	***MANAGEMENT – CUSTOM METRICS:*** *Does the cloud provider's monitoring service allow users to create and monitor custom metrics?*
4.	***MANAGEMENT – MONITORING GRANULARITY:*** *Does the cloud provider's monitoring service provide various levels of monitoring granularity, down to the 1-minute level?*
5.	***MANAGEMENT – API TRACKING SERVICE:*** *Does the cloud provider offer a service that logs, monitors, and stores activity against cloud resources both at the console and at the application programming interface (API) level for improved visibility?* • *If yes, what are the cloud provider's services that integrate with this tracking service?*
6.	***MANAGEMENT – NOTIFICATION:*** *Does the cloud provider enable the capability of sending out notifications based on application programming interface (API) activity levels?*
7.	***MANAGEMENT – COMPRESSION:*** *Does the cloud provider offer a mechanism to compress logs generated by the application programming interface (API) tracking system in order to help users reduce storage costs associated with this service?*

8.	*MANAGEMENT – REGION AGGREGATION:* *Does the cloud provider offer the capability of recording account application programming interface (API) activity in all regions and deliver this information in an aggregated fashion for ease of use?*
9.	*MANAGEMENT – RESOURCE INVENTORY:* *Does the cloud provider offer a service to assess, audit, and evaluate the configurations of resources deployed by a user?*
10.	*MANAGEMENT – CONFIGURATION CHANGES:* *Does the cloud provider automatically record a resource configuration change when it happens?*
11.	*MANAGEMENT – CONFIGURATION HISTORY:* *Does the cloud provider offer the ability to examine resources configuration at any single point in the past?*
12.	*MANAGEMENT – CONFIGURATION RULES:* *Does the cloud provider offer guidelines and recommendations for provisioning, configuring, and continuously monitoring compliance?*
13.	*MANAGEMENT – RESOURCES TEMPLATES:* *Does the cloud provider offer users the capability of creating, provisioning, and managing a collection of resources in a template-like fashion?*
14.	*MANAGEMENT – RESOURCES TEMPLATES REPLICATION:* *Does the cloud provider offer the ability to quickly replicate these resource templates across different regions to be potentially used in disaster recovery (DR) situations?*
15.	*MANAGEMENT – TEMPLATE DESIGNER:* *Does the cloud provider offer an easy-to-use graphical tool with drag-and-drop functionality that speeds up the process of creating such resource templates?*
16.	*MANAGEMENT – SERVICE CATALOG:* *Does the cloud provider offer a service to create and manage a catalog of services, i.e., servers, virtual machines, software, databases, etc.?*
17.	*MANAGEMENT – CONSOLE ACCESS:* *Does the cloud provider offer a web-based user interface to facilitate management and monitoring of cloud services?*
18.	*MANAGEMENT – CLI ACCESS:* *Does the cloud provider offer a unified tool to manage and configure multiple cloud services from the command line interface (CLI) and allow to automate management tasks through the use of scripts?*
19.	*MANAGEMENT – MOBILE ACCESS:* *Does the cloud provider offer a smartphone application to allow users to connect to the cloud service and manage their resources?* • *If yes, is this application available for both iOS and Android?*
20.	*MANAGEMENT – BEST PRACTICES:* *Does the cloud provider have a service that helps users compare their cloud usage against best practices?*
21.	*MANAGEMENT – SERVICE LIMITS:* *Does the cloud provider have any restrictions (i.e. service limits) in regards to the management section above?* *Example:* *Maximum number of configuration rules per account*

	Maximum number of alarms that can be created *Maximum number of logs that can be stored*

10. Support

	Requirement
1.	***SUPPORT – SERVICE:*** *Does the cloud provider offer support at any time, 24 hours a day, 7 days a week, and 365 days per year via phone, chat, and email?*
2.	***SUPPORT – SUPPORT TIERS:*** *Does the cloud provider offer different support tier levels?*
3.	***SUPPORT – TIER ALLOCATION:*** *Does the cloud provider allow users to self-assign the resources/services consumed to different levels of support based on granular classification, and not by forcing users to maintain separate cloud accounts to achieve and receive different levels of support?*
4.	***SUPPORT – FORUMS:*** *Does the cloud provider offer public support forums for customers to discuss their issues?*
5.	***SUPPORT – SERVICE HEALTH DASHBOARD:*** *Does the cloud provider offer a service health dashboard that displays up-to-the-minute information on service availability across multiple regions?*
6.	***SUPPORT – PERSONALIZED DASHBOARD:*** *Does the cloud provider offer a dashboard that displays a personalized view into the performance and availability of the services underlying user's specific resources?*
7.	***SUPPORT – DASHBOARD HISTORY:*** *Does the cloud provider offer 365 days' worth of service health dashboard history?*
8.	***SUPPORT – CLOUD ADVISOR:*** *Does the cloud provider offer a service that acts like a customized cloud expert and helps compare resources' usage against best practices?*
9.	***SUPPORT – TAM:*** *Does the cloud provider offer a technical account manager (TAM) that provides technical expertise for the full range of cloud services?*
10.	***SUPPORT – THIRD-PARTY APPLICATION SUPPORT:*** *Does the cloud provider offer support for common operating systems and common application stack components?*
11.	***SUPPORT – PUBLIC API:*** *Does the cloud provider offer a public application programming interface (API) that programmatically interact with support cases to create, edit, and close such cases?*
12.	***SUPPORT– SERVICE DOCUMENTATION:*** *Does the cloud provider offer good quality, publicly-viewable technical documentations for all its services including, but not limited to user guides, tutorials, frequently Asked questions (FAQs), and release notes?*
13.	***SUPPORT– CLI DOCUMENTATION:***

	Does the cloud provider offer good quality, publicly-viewable technical documentation for its command line interface (CLI)?
14.	***SUPPORT– REFERENCE ARCHITECTURES:*** *Does the cloud provider offer a free, online collection of reference architecture documents to help customers build specific solutions combining many of cloud provider's cloud services?*
15.	***SUPPORT– REFERENCE DEPLOYMENTS:*** *Does the cloud provider offer a free, online collection of documents containing detailed, tested and validated, step-by-step procedures, including best-practices, to implement common solutions (i.e. DevOps, Big Data, Data Warehouse, Microsoft workloads, SAP workloads, etc.) in its cloud offerings?*

Appendix B – Live Technical Evaluation

When selecting a CISP, it is important to assess cloud platform capabilities 'live' using the CISP's publicly available services and infrastructure. We recommend at least 1 full day per shortlisted CISP for technical evaluation. During the evaluation you can: 1) Conduct an in-depth evaluation to assess whether the demonstrated capabilities align with your RFP requirements and the CISP's written responses, 2) Provide a platform for your experts to probe the CISP to ensure fit and alignment with your specific technical and organizational needs, and 3) Gain confidence in CISP Services and the CISP's ability to scale, operate securely, operate resiliently, and continue to innovate to meet future needs.

When CISPs respond to the requirements of a Cloud Services RFP, they may state compliance based on a high-level interpretation of requirements, which lacks the full context of an organization's operating environment/application needs. We recommend staffing a live technical evaluation panel with leading technical, operational, security and application experts. Evaluators should challenge the CISP throughout the evaluation, and as a best practice they should score CISPs independently, rating scenarios on a set scale, such as 0–4 (0=Unacceptable, 1=Marginal, 2=Acceptable, 3=Good, 4=Outstanding). Afterwards, the demo scores can be consolidated, with the average score for each evaluation scenario rolled up to the overall CISP evaluation. Scenarios with a high standard deviation should be discussed as an evaluation team prior to finalisation. Once scores are consolidated, a weighting based on the criticality of the scenarios can be applied.

In terms of the demonstration scope, we recommend taking a holistic view of the CISP's platform, and then diving deeper to evaluate specific workloads running on the platform. Below is a sample outline of a platform and workload evaluation. Organizations can build upon this baseline or customise it to ensure that the selected CISP meets their specific functional and non-functional requirements. As a best practice, suppliers presented with the list of scenarios and requirements can be allowed to propose an agenda for the live evaluation that maximises coverage and includes 20% Q&A time.

Platform Evaluation: Multiple CISPs have adopted the term 'Well Architected' to refer to an approach to cloud that delivers optimal value and minimizes risk. Well Architected scenarios in a live technical demonstration can include:

1. **Security:** Identity, Centralised Governance, Automated Threat Detection, Data Protection, Event Readiness
2. **Performance Efficiency:** Right Sizing, Scalability/Elasticity, Serverless
3. **Reliability:** High Availability (Resilience to failures), Reduce risk of Change, Disaster Recovery, Backup
4. **Cost Management:** Financial Operations, Commercial Optimisation, Budgets and Cost Allocation
5. **Operational Excellence:** Automation, Monitoring, Support, Management and Capabilities required to migrate to and operate within the cloud

Workload Evaluation: A common set of application types that can be demonstrated include:

- **Web Application:** Publicly hosting a dynamic website, including back-end database and static object storage.
- **Data Analytics:** A Data Lake or Lake House architecture that enables the consolidation of data from disparate data providers and the ability to deal with high Volume (TBs / PBs of data), Variety (Structured, unstructured, different formats etc.) and Velocity (Rate of data generation, change and query patterns).
- **Data Science Platform:** A platform that enables the development, deployment and use of AI/ML-based capabilities across your organization.
- **IoT Application:** An IoT platform/capability that spans the cloud, a network capability and the devices.

For each representative workload that is important to your organization, you can define the scenarios to be demonstrated by the CISP. The scenarios should demonstrate overall capabilities that enable the deployment of the workload in a Well Architected way. The following pages include sample Live Technical Evaluation criteria for; 1) the CISP's Platform, and 2) a sample Web Application workload.

Platform – Sample Live Technical Evaluation

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
Plat.Sec.1	Identity Federation	4	Demonstrate the ability to federate from an existing identity store to the cloud service.	• Support for standard protocols such as SAML. • Support for SCIM-based identity replication. • The ability to define different access levels within the corporate identity store and have those applied within the cloud provider. • The ability to limit specific teams/individuals only to certain accounts/projects/workloads. • Ability to support Attribute-Based Access Control (ABAC) and use those attributes within the cloud provider Identity and Access Management (IAM) system to control access to cloud resources.
Plat.Sec.2	Central Governance	4	Demonstrate the ability to define policy and requirements centrally, at an organizational level (Global policies) and also at a business unit and project level.	• Policy should include: Enable/disable services, Apply geographical restrictions (limit regions). • The policies should also restrict users, including administrators, from disabling any auditing/governance controls.
Plat.Sec.3	User Permission Limitation	3	Demonstrate the automatic recommendations for tightening of user permissions.	• Ability to compare current permissions with required permissions. • Automatic generation of policies to promote least privilege.
Plat.Sec.4	Audit Logging	4	Demonstrate audit logging of cloud activity, including both allowed and disallowed actions.	• Centralised logs for the whole organization. • Account/Project specific logs to support low level tracking and accountability. • Tools to enable the querying of logs. • Tools that enable triggering actions based on specific events/log entries. • Ability to view supplier support activity. • Ability to prevent deletion of logs, even by administrators.
Plat.Sec.5	Network Isolation	4	Demonstrate and evidence where possible the isolation of different tenants within the cloud. Demonstrate the configuration of isolated (without connectivity), private	• Separation of tenants, including on VPN and cross-connection services. • Ability to control traffic flow from outside the cloud infrastructure (on-prem), within it and to the Internet.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
			(with no Internet) and public (with Internet access) subnets.	• How the separation applies when using shared services such as container hosting or function as a service.
Plat.Sec.6	Encryption at rest	4	Demonstrate the ability to encrypt data at rest, including the options for BYOK and client-side encryption.	• Ability to require encryption for sensitive data. • Ability to use either provider managed keys or customer managed keys. • Adherence to FIPS 140-2. • Ability to alert for and log mal-adherence to encryption requirements. • Additional cost impact. • Performance impact. • Support for quantum proof algorithms and key sizes.
Plat.Sec.7	Encryption in transit	4	Demonstrate the ability to encrypt data in transit.	• Encryption by default for service APIs. • Ability to enable encryption in transit (TLS) on load balancers and managed APIs. • Support for mutual (client and server) authentication.
Plat.Sec.8	Key Management	4	Demonstrate your Key Management capability. Include the full key life-cycle. Include integration with cloud services.	• Logging creation, use of, rotation and destruction of keys.
Plat.Sec.9	Configuration Management	3	Demonstrate your configuration management capabilities of the cloud platform.	• Maintain accurate CMBD. • Check for compliance. • Trigger actions based on non-compliance automatically. • Ability to evaluate configuration changes against best practice or custom rules.
Plat.Sec.10	Network Security	3	Demonstrate the Web Application Firewall and Firewall capability, including integration with 3rd party rule sets / firewalls and volumetric attack protection.	• WAF (Web Application Firewall) capabilities: Scalability. • Private as well as Public network support. • Ability to subscribe to industry/vendor feeds for rule sets. • Automatically trigger actions within the infrastructure based on events from the WAF. • Firewall capabilities, Scalability. • Host-based and Network-based firewalls. • Ability to reference logical groups or objects in addition to the ability to specify CIDR IP Blocks. • Number of rules supported at each level / component.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
				• Ability to support a distributed operating model (Network team + Dev team) through policy and network configuration.
Plat.Sec.11	Network Connectivity	3	Demonstrate the ability to connect to on-prem networks as well as endpoints/clients to private networks within the cloud.	• Private connectivity (high bandwidth > 10GBs). • Ability to control routing and firewall policies across the organization. • VPN Connectivity (site-to-site and client-based). • IPV6 Support.
Plat.Sec.12	Instance Management	3	Demonstrate instance management capabilities.	• Ability to monitor and manage patch state of a large volume of instances. • Support for Linux and Windows Operating system patch management. • Ability to execute commands across a fleet of servers without the need for SSH. • Ability to control and audit remote access to virtual machines centrally. • Ability to change an instance size, attach additional volumes, change network configuration etc. via Console, CLI and API.
Plat.Sec.13	Policy application	3	Demonstrate the ability to configure services to prevent access from the public Internet.	• Ability to isolate traffic to private networking for services likely to contain critical/confidential data. • Ability to define policies that control access to data based on the source network. • Application of these access restrictions to all users, including users with high level credentials.
Plat.Sec.14	Vulnerability scanning	2	Demonstrate the ability to scan images (container and VM) for vulnerabilities.	• Ability to automatically scan Containers in a registry. • Ability to scan virtual machines for known vulnerabilities. • Ability to perform network scanning.
Plat.Sec.15	Network Inspection	2	Demonstrate the ability to capture/mirror network traffic (NetFlow and full packet) from within a customer environment.	• Ability to mirror some/all of the traffic within the cloud provider infrastructure (from a customer tenant perspective), including full packet capture. • Ability to simply select which traffic you want to capture. • Ability to scale to very large traffic volumes (>50GBps).

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
Plat.Sec.16	Threat Detection	3	Demonstrate the Intrusion detection capability of your platform, including threats from a network, credential use and usage pattern analysis for example.	• Ability to detect suspect activities like “mining”. • Ability to detect brute for authentication attacks like SSH logins. • Ability to detect credential leakage or abuse. • Application of ML, analysing large numbers of event and surfacing prioritised events. • Effort to enable/configure (simple is better). • Ability to integrate with external services and trigger notifications. • Ability to configure the IDS at a global level for all projects/accounts.
Plat.Perf.1	Compute Optimisation	2	Demonstrate automatic recommendations for optimisation of Virtual Machine and Function as a Service costs.	• Recommendations based on actual utilisation and workload patterns. • Recommendations include estimated savings and insights into expected load level/technical implications. • Optimisations should include both savings and "performance risk" where virtual machines may for example be under-sized.
Plat.Perf.2	Environment Optimisation	2	Demonstrate automatic recommendations for other cloud components such as load balancers, networking, databases, storage etc.	• Recommendations identify savings and potential performance efficiency opportunities in other components beyond core compute.
Plat.Perf.3	Compute Auto-Scaling	4	Demonstrate the automatic scaling capabilities of an application deployed behind a load balancer in a virtual compute environment. Demonstrate the different options / approaches available and the ability to trigger other (optional) actions before/after scaling events, such as a notification.	• Different options for scaling, trigger-based, time-based, manually or more intelligent approaches that apply machine learning to predict required capacity. • Fully automated scaling, including registration with a load balancer and health checks. • The ability to execute an arbitrary piece of code at specific points of the scaling lifecycle.
Plat.Perf.4	Online Scaling for Storage	3	Demonstrate the ability to scale both capacity and throughput of block storage without interruption to the workload.	• Ability to transition block storage between different storage types without the need to rebuild services completely. • Ability to increase the size of volumes presented to VMs.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
Plat.Perf.5	Auto-Scaling for Managed Services	3	Demonstrate the ability for the Object Store, API Gateway, FaaS platform and NoSQL database to scale from few (10s) to many (1000s) of concurrent users.	• Seamless auto-scaling, ideally without administrator intervention. • Consistent performance during a ramped scaling up period that aligns with production scaling requirements. • For some components, like FaaS, look at options for pre-warming and managing concurrent execution limits if needed as well.
Plat.Perf.6	Container-based workloads	3	Demonstrate the ability to host container-based workloads.	• Options for container hosting platforms. • Integration with other IaaS components such as load balancers. • Availability of a service mesh solution. • Non-proprietary options for container hosting, such as Kubernetes. • Native support for high availability within the Container control-plane. • Ability to manage on-prem container hosts.
Plat.Rel.1	Regional Resilience	4	Demonstrate the automated failover of a relational database instance within a region when a geographically localised failure (such as a power outage) is simulated.	• Automated failover. • Isolated fault zones within a cloud region. • Clearly demarcated and simple to architect for High Availability.
Plat.Rel.2	Instance Auto-recovery	2	Demonstrate the auto-recovery of an instance / set of instances following a failed health check.	• Configurable health checks. • Fully automated instance recover/re-provisioning.
Plat.Rel.3	Load Balancer Health Awareness	3	Demonstrate how a load balancer automatically detects a faulty instance and re-routes traffic to other healthy hosts.	• Configurable health checks. • Automated traffic routing to healthy hosts.
Plat.Rel.4	Region failover	3	Demonstrate a multi-region architecture, including automated traffic shift to a secondary region.	• Globally aware health checks. • Automated routing options: latency, weighed and failover. • Support for Virtual Machine workloads as well as managed services like an Object Store / NoSQL database service.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
Plat.Rel.5	Backup and Recovery	4	Demonstrate the Backup and Recovery options for: Virtual Machines, Databases, Managed services.	• Level of automation. • Ability to restore to the same / another cloud region. • Ability to copy backups to another cloud region.
Plat.Cost.1	Budgets	3	Demonstrate a budget management capability, including how to structure it for sub-accounts and projects.	• Consider the ability to apply budgetary controls and monitoring at the different levels of your organization. • Check for flexibility, for example to the ability to group components (through tagging), set budgets for specific cloud services, and configure thresholds for alerting/monitoring.
Plat.Cost.2	Budget Allocation	1	Demonstrate the provision of a new project environment (account), including the budget allocation process for the project. The provisioning should include manual approval steps for 1) Technical review/IT, 2) Commercial review/Finance.	• The ability to self-provision, with the appropriate approvals. • Automation of the configuration of the appropriate budget setting, notifications or budget policies as appropriate for your organization.
Plat.Cost.3	Budget Reporting	2	Demonstrate the capability to report on budgets across the organization. Reporting for a specific department vs. the whole organization (need to know). Reporting should include "actual" as well as forecasted/estimated spend values.	• The ability to provide visibility at different levels of the organization, creating awareness and transparency, but on a need-to-know basis. • Forecasting should be based on current and past consumption trends and provide early warning of potential budget over-runs.
Plat.Cost.4	Budget Controls	1	Demonstrate the ability to take actions when a budget threshold is reached. Actions could include notifications, applying constraints or active intervention to prevent budget over-spend.	• The ability to define actions simply to different projects. • The ability for the actions to vary from one project to another, for example - taking into account Dev vs. Prod implications. • The ability to define multiple actions and thresholds for the same budget/project. • The ability to define custom actions in additional to standard capabilities.
Plat.Cost.5	Budget Periodicity	1	Demonstrate the ability to apply budgets for different time periods, daily/monthly/yearly etc. For yearly budgets, demonstrate the ability to apply a	• Ability to define budgets for different time periods. • Ability to configure a distribution of spend across the year for annual budgets, especially important for seasonal/highly elastic workloads such as an annual tax return for example.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
			variable distribution of expected spend throughout the year.	
Plat.Cost.6	3rd Party Marketplace	3	Demonstrate the ability to buy and deploy 3rd party products. Demonstrate how to set a budget for a set of 3rd party products available via a marketplace and also the ability to restrict the available products.	• Ability to set a budget for a specific product; a global budget, a budget for a set of projects/accounts. • Ability to only present a sub-set of the broader marketplace to cloud users.
Plat.Cost.7	Compute pricing models	3	Demonstrate the different pricing/commercial models that can be applied to virtual machines.	• Capabilities should include on-demand, with no required long term commitment and granular (per minute/hour) pricing. • Optional long term commitments in return for a discount. • Ability to buy instances with a willingness to be interrupted in return for a discount. • Importantly, it should be possible to mix these models within the same project/accounts, and also to share benefits across different accounts.
Plat.Cost.8	Commercial Optimisation Recommendations	3	Demonstrate the ability to receive commercial optimisation recommendations to optimise spend (without having to make technical changes).	• Holistic recommendations for multiple services, including for example Virtual Machines and Managed Databases. • Ability to action recommendations simply and understand the expected savings/benefit.
Plat.Cost.9	Dedicated Hosts	4	Demonstrate the ability to provision a dedicated host to enable the use of on-premises licensing that are tied to a specific host.	• Ease of provisioning. • Ability to manage the utilisation of the host. • The ability to share the host across different projects/tenancies.
Plat.Ops.1	Virtual Machine Migration	3	Demonstrate the import of a virtual machine from on-premises to a cloud-based VM service.	• Ability to import both Windows and Linux-based operating systems. • Ability to import multiple machines at once. • Ability to maintain a replication session to enable rapid "failover" to cloud.
Plat.Ops.2	DevOps and Automation Capabilities	4	Demonstrate your DevOps / automation capabilities including how environments are defined as code, support from fully	• Ability to define all systems components as code, including network, virtual machines, storage, databases. • Ability to create a pipeline. • Ability to create a code repository.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
			automated deployments, automated testing and rollbacks.	• Ability to automate builds. • Ability to perform blue/green deployments. • Ability to create multiple environments and have multiple stages for deployments. • Automated rollback for failed deployments
Plat.Ops.3	Application Hosting	2	Demonstrate the hosting of a simple 2-tier application in a low-code/platform service. Including a relational database and auto-scaling for the application/web tier.	• Simple configuration via the UI. • Inclusion of health checks, scaling, high availability. Platform support, Windows and Linux.
Plat.Ops.4	Security Integration	2	Demonstrate the integration capabilities of your platform from the perspective of Security Incident and Event Management.	• Ability to easily integrate and consume security related logs from the cloud provider + APIs for integration.
Plat.Ops.5	ITSM Integration	3	Demonstrate the integration capabilities of your platform from the perspective of an ITSM (IT Service Management) perspective.	• Ability to raise, monitor and update a support case through an API. • Ability to provision services or sets of services as "products" through an API.
Plat.Ops.6	Support	4	Demonstrate your support offering.	• Different levels of support for different types of workloads. • Ability to also support the Operating System / Database Engine etc. as appropriate for a given service. • Ability to offer a white glove offering with named support leads for critical workloads. • Ability to offer a structured event readiness and architecture review process. • Insight into the provider roadmap.
Plat.Ops.7	Auditability	4	Demonstrate the tooling that you have to support compliance audits.	• Ability to obtain compliance audit details via the console. • Ability to manage and automate environment audits.
Plat.Ops.8	VM to Container	1	Demonstrate the conversion of an application on a virtual machine to a container, and serving it using the cloud provider container platform.	• Ease of use of the conversion. • Time to convert. • Platform support, .Net and Java.

Workload: Web Application – Sample Live Technical Evaluation

The following section provides a sample workload evaluation sheet for a specific "Web Application" workload. When developing an evaluation sheet for a given application, it is strongly recommended to involve the application users, developers and administrators as they are likely to have the best understanding of the requirements, current challenges and constraints.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
Web.Sec.1	Security – Application Protection	3	Demonstrate your ability to block malicious attempts to exploit the application through SQL Injection, XSS Scripting attack and other attacks.	• Ability to protect against common attacks "out of the box" with standard rules/capabilities. • Ability to create custom checks/rules/functions.
Web.Sec.2	Security –Rate-based Protection	3	Demonstrate your ability to block/protect against attacks involving large request rates or data volumes directed at an application.	• Ability to configure limits and restrict request rates from a given IP address or list of addresses.
Web.Sec.3	Security – Source-based Protection	3	Demonstrate the ability to restrict access based on network / geographical source.	• Ability to restrict by network block or a list of network blocks. • Ability to restrict by origin Country (without the need to manage IP lists).
Web.Sec.4	Security – Network Segmentation	4	Demonstrate the ability to isolate/protect components (Web Server, App Server / DB Server) to protect against both North-South and East-West propagation through the infrastructure.	• Ability to place components in different subnets and control traffic flow between different subnets. • Ability to control traffic flow at a network interface level. • Ability to reference logical groups as well as CIDR blocks.
Web.Sec.5	Security – TLS Support and Certificate Management	4	Demonstrate the ability to deliver a TLS-secured endpoint and automatically manage the supporting components to deliver that, including for example the automatic rotation of certificates.	• Support for the latest TLS protocols and the ability to disable legacy versions if required. • Simple certificate generation, management and rotation (ideally fully automated).
Web.Perf.1	Performance - Scalability	4	Demonstrate your ability to scale from 10 to 100,000 concurrent users of the web application through dynamic auto-scaling.	• Ability to defined time-based as well as trigger-based scaling rules. • Seamless scaling for the end user and administrator. Automatically scaling out when load increases and scaling in when load decreases.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
				• Ensure that scalability exists at each layer of the web application (Load Balancer, Web Layer, Data Layer etc.). • The availability to caching services at different layers of the application as appropriate.
Web.Perf.2	Performance - Global Delivery	3	Demonstrate your CDN capability including demonstrating latency from different points around the globe, including: Australia, Asia, Africa, Middle East, North America, South America and Europe.	• Ability to create and configure a CDN through the CISP console/APIs. • Configurable distribution rules for different geographies. • Configurable caching for different use cases /applications.
Web.Rel.1	Reliability – Single-Region Resilience	4	Demonstrate the ability to tolerate a localized event such as a loss of network connectivity to the CISP data centre.	• Automated failover and high availability within a cloud region (City).
Web.Rel.2	Reliability - Multi-Region Deployment	3	Demonstrate a multi-region deployment of a web application including a globally replicated database.	• Ability to deploy a multi-region application programmatically. • Replication between the regions for the data store. • Automated routing of users to their optimal region.
Web.Rel.3	Reliability – Multi-Region Failover	3	Demonstrate the automatic failover of a web application in the case of a regionally impacting service problem.	• Automated failover and high availability across multiple cloud regions.
Web.Cost.1	Cost – Visibility	2	Demonstrate the ability to track cost per application	• Ability to view historical costs for a specific application, including when it scales up / down.
Web.Cost.2	Cost – Budgets	2	Demonstrate the ability to set budgets and related alerts per application.	• Budgets configured per application and the ability to trigger actions / alerts based on configured thresholds.
Web.Ops.1	Ops – Maintenance Windows	3	Demonstrate the ability to configure maintenance windows to align with business requirement, especially where maintenance may impact application availability.	• Configurable maintenance windows for components like a relational database service.
Web.Ops.2	Ops – Logging	3	Demonstrate the ability to centralise logging for an application with multiple components, including persistence of logs upon termination/failure of virtual machines.	• Ability to configure centralized logging service that can scale along with the application requirements. • Ability to define rules/filters to trigger alerts or actions based on specific log events.

Scenario ID	Scenario Name	Criticality (1=Low, 4=Critical)	Demonstration Requirements	Scoring Considerations
Web.Ops.3	Ops - Monitoring	3	Demonstrate monitoring of the application, including performance, availability, response times, error counts etc. and functionality to take action/trigger notifications based on different metric thresholds.	• A collection of standard metrics available such as disk IO, CPU, Database metrics, Network, Load balancer etc. • Ability to define custom metrics, thresholds. • Ability to create a custom dashboard to represent the most important metrics and share those dashboards with relevant users.