



GOVERNANCE

GOVERNANCE

EQUITABLE GROWTH, FINANCE & INSTITUTIONS INSIGHT

Institutional and Procurement Practice Note on Cloud Computing

Cloud Assessment Framework and Evaluation Methodology

World Bank Advisory Services and Analytics

Supported by the GovTech Global Partnership - www.worldbank.org/govtech



WORLD BANK GROUP

GovTech
Putting people first

© 2023 International Bank for Reconstruction and Development / The World Bank
1818 H Street NW,
Washington DC 20433
Telephone: 202-473-1000;
Internet: www.worldbank.org

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent.

The World Bank does not guarantee the accuracy, completeness, or currency of the data included in this work and does not assume responsibility for any errors, omissions, or discrepancies in the information, or liability with respect to the use of or failure to use the information, methods, processes, or conclusions set forth. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be construed or considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, all of which are specifically reserved.

Rights and Permissions

The material in this work is subject to copyright. Because The World Bank encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given.

Any queries on rights and licenses, including subsidiary rights, should be addressed to World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433, USA; fax: 202-522-2625; e-mail: pubrights@worldbank.org.



Contents

Acknowledgments	v
List of Acronyms	vii
Executive Summary	1
1. Introduction	7
1.1 Cloud Service Models	8
1.2 Cloud Deployment Models	10
1.3 Cloud Security Accreditations and Certifications	13
1.4 Report Objective	13
2. Lessons Learned: A Comparative Analysis of Case Studies	14
2.1 Institutional Coordination Mechanisms	15
2.1.1 Cloud First Principle	15
2.1.2 Top-Level Policies and Strategies	16
2.1.3 Institutional Framework	16
2.2 Data Classification and Security Framework	18
2.2.1 Data Classification	18
2.2.2 Data Residency Requirements	19
2.2.3 Security Controls	19
2.2.4 Security Assessments	20
2.2.5 Continuous Monitoring	21
2.3 Procurement Arrangements	21
2.3.1 Finding and Selecting Cloud Services	21
2.3.2 Managing Vendor Lock-in	23
2.3.3 Payment Methods	24
3. The Way Forward – Main Takeaways	25
Appendix 1: Step-By-Step Guide to Public Cloud Assessments and Procurements for Government	33
Appendix 2: Comparison Table of Case Studies	35
Annex 1: Japan’s ISMAP Program	38
Annex 2: Australia’s Anatomy of a Cloud Assessment and Authorization Framework	47
Annex 3: UK’s Digital Marketplace and G-Cloud Framework	58

Annex 4: South Africa’s Cloud Security Framework	66
Annex 5: Dubai’s Cloud Security Risk Management Approach and Procedures	73
Notes	80
References	88

Boxes

Box 3.1. Suggested Language for a Cloud First Policy	26
Box 3.2. How Cybersecurity Concerns in Ukraine Led to the Migration of Government Data to Public Cloud	27
Box 3.3. Data Migration Considerations – Lessons from Singapore	30
Box 3.4. Considerations for a Call-Off Contract Template for a Cloud Marketplace	31

Figures

Figure 1.1. Cloud Service Models	8
Figure 1.2 Shared Responsibility between Consumer and CSP	9
Figure 1.3. Example Services Available to a Cloud Consumer (NIST SP 500-292)	10
Figure 1.4. Types of Cloud Deployment	11
Figure 1.5. Different Cloud Deployment Schemes	12
Figure 2.1. Comparison of Data Classification Levels	18
Figure 2.2. Comparison of Case Studies’ Data Residency Requirements	19
Figure 2.3. Portability and Value Considerations for Cloud Services	23
Figure A1.1. Basic Framework of ISMAP	41
Figure A1.2. Structure of ISMAP’s Control Criteria	43
Figure A1.3. Four-Step Process of ISMAP	45
Figure A2.1. Notional Framework of Australia’s Institutional Mechanisms for Secure Cloud Procurements	50
Figure A2.2. Australian Government’s Data Classification System (PSPF Policy 08 – Sensitive and classified information)	51
Figure A2.3. Phase 1 of the Cloud Assessment Process for Australian Procuring Agencies	55
Figure A2.4. Phase 2 of the Cloud Assessment Process for Australian Procuring Agencies	56
Figure A3.1. Notional Framework of the UK’s Institutional Mechanisms for Secure Cloud Procurements	61
Figure A3.2. The UK’s Data Classification System	62

Figure A3.3. NCSC's Four-Step Process for Procuring Public Cloud Services	64
Figure A4.1. Notional Framework of the South Africa's Institutional Mechanisms for Secure Cloud Procurements	68
Figure A5.1. Notional Framework of the Dubai's Institutional Mechanisms for Secure Cloud Procurements	75
Figure A5.2. Categories of Dubai Data	76
Figure A5.3. CSP Security Standard Certification Process	78

Tables

Table ES.1. Major Similarities and Variations in Case Studies	2
TABLE 2.1. Benchmarking the Case Studies using the GTMI (updated October 2022), the EGDI (updated 2022), and the Global Cloud Ecosystem Index (updated 2022)	15
Table 2.2. Summary of Institutional Frameworks of the Case Studies	17
Table 2.3. Comparison of Security Assessment Considerations and Activities	20
Table 2.4. Summary of Procurement Models of the Case Studies	22
Table 3.1. Example of a Responsibility Matrix for Institutional Framework of Cloud Preapproval and Procurement	26
Table A2.1. ISM Security Control Principles	53
Table A3.1. NCSC's 14 Cloud Security Principles	60
Table A4.1. Key Considerations for South African Procuring Agencies under the Determination and Directive	70



Acknowledgments

This note has been developed under the World Bank GovTech Global Partnership by a team led by Khuram Farooq (Senior Governance Specialist). The World Bank team was composed of Hunt La Cascia (Senior Public Sector Specialist); Knut Leipold (Lead Procurement Specialist); and Bertram Boie (Senior Digital Development Specialist); Robert Shields (Consultant); and Constantine Pagedas (Consultant). Overall guidance for the report was provided by Tracey Marie Lane (Practice Manager, Governance GP); Edward Olowo-Okere (Senior Advisor, EFI VP); Arturo Herrera Gutierrez (Global Director, Governance GP); and Donna Andrews (Acting Practice Manager, Governance GP).

The note benefited from the expertise of the following World Bank experts: Natalija Gelvanovska-Garcia (Senior Digital Development Specialist), Dolele Sylla (Senior Governance Specialist) and Ishtiaq Siddique (Senior Procurement Specialist).

The note also benefited from the expertise of the following individuals: Matt Jodlowski (Australia, Policy Lead, Digital Strategy, Digital Transformation Agency); Bushra Al Blooshi (UAE, Research and Innovation Head, Dubai Electronic Security Center, Digital Dubai); Ben Vandersteen (United Kingdom, Technical Architect, Government Digital Service); Ayanda Nkundla (South Africa, Senior Manager, ICT Compliance, Department of Public Service and Administration); Alufheli Swalivha (South Africa, Director, Public Service ICT Stakeholder Management, Department of Public Service and Administration); Zaid Aboobaker (South Africa, Chief Director, E-Government, Department of Public Service and Administration); and various officials from Japan's Information-technology Promotion Agency.

The following members of a Cloud Computing Working Group initiated by the World Bank GovTech initiative contributed their expertise: Cheow Hoe Chan (Singapore, Government Chief Digital Technology Officer, GovTech Singapore); Richard Tay (Singapore, Head for the Whole-of-Government Operations, GovTech Singapore); Karen Kee (Singapore, Deputy Director, GovTech Singapore); Ben Vandersteen (United Kingdom, Technical Architect, Government Digital Service); Liz Lutgendorff (United Kingdom, International Lead Insight and Analysis Advisor, Government Digital Service); Abhishek Singh (India, President and CEO, National eGov Dept, Ministry of Electronics and IT); Bramhanand Jha (India, Sr. Consultant, Program Management, Ministry of Electronics and IT); Vinay Thakur (India, COO, National eGovernance Division, Ministry of Electronics and IT); Rachel Ran (Israel, Head of Cloud Strategy, National Digital Agency); Keren Katsir Stiebel (Israel, CMO, Director of Marketing, Communications and Foreign

Affairs, Government ICT Authority); Toshiyuki Zamma (Japan, Head of International Strategy, Digital Agency); Kensuke Yabata (Japan, Director, Digital Agency); Sungjoo Son (South Korea, Director, Ministry of the Interior and Safety); Erica Dubach (Switzerland, Head of Division on Transformation and Interoperability, Swiss Federal Chancellery); Philippe Bruegger (Switzerland, Project Manager, SECO); Natalie Bertsch (Switzerland, Project Manager, SECO); Bushra Al Blooshi (UAE, Research and Innovation Head - Dubai Electronic Security Center, Digital Dubai); Ahmed AlSalman (UAE, Senior Manager Cloud Services, The Telecommunications and Digital Government Regulatory Authority); Omar Alriyami (UAE, Director, Data Analysis and Engineering, Statistics Centre, Abu Dhabi); Aziz Alkayyoomi (UAE, Acting Director of Information Technology, Statistics Centre, Abu Dhabi); and Maximiliano Maneiro (Uruguay, Emerging Technologies Manager, Electronic Government and Information and Knowledge Society Agency).

Richard Crabbe provided editorial services, and Maria Lopez designed the final publication.

This report was made possible by the World Bank's GovTech Initiative and the GovTech Global Partnership trust fund, building on support of financial and in-kind partners that include the Ministry of Finance of Austria, the State Secretariat for Economic Affairs (SECO) of Switzerland, the Ministry of Economy and Finance (MOEF) of the Republic of Korea, the Ministry of Economic Development of the Russian Federation, the Ministry of Interior and Safety (MOIS) of the Republic of Korea, the Government of Japan and the Federal Ministry for Economic Cooperation and Development (BMZ) of Germany.



List of Acronyms

ASD	Australian Signals Directorate
ACSC	Australian Cyber Security Centre
AO	Authorizing Officer
CCCS	Canadian Center for Cyber Security
CCS	Crown Commercial Service (UK)
CCSL	Certified Cloud Services List (Australia)
CDDO	Central Digital and Data Office (UK)
CIA	Confidentiality, Integrity, and Availability
COTS	Commercial-off-the-shelf
CSCM	Cloud Security Controls Matrix (Australia)
CSA	Cloud Security Alliance
CSO	Cloud Service Offering
CSCP	Cloud Services Certification Program (Australia)
CSP	Cloud Service Provider
DCDT	Department of Communications and Digital Technologies (South Africa)
DDA	Dubai Digital Authority
DDE	Dubai Data Establishment
DESC	Dubai Electronic Security Center
DSC	Dubai Statistics Center
DTA	Digital Transformation Agency (Australia)
DPSA	Department of Public Service and Administration (Australia)
ECTA	Electronics Communications and Transaction Act (South Africa)
FedRAMP	Federal Risk and Authorization Management Program (United States)
GDS	Government Digital Service (UK)
GDPR	General Data Protection Regulations
HCF	Hosting Certification Framework (Australia)
HOD	Head of Department (South Africa)
IaaS	Infrastructure as a Service

ICT	Information and Communications Technology
IPA	Information-technology Promotion Agency
IRAP	Infosec Registered Assessors Program (Australia)
ISMAP	Information System Security Management and Assessment Program (Japan)
ISM	Information Security Manual (Australia)
ISO/IEC	International Standards Organization and the International Electrotechnical Commission
ISR	Information Security Regulation (Dubai)
JASA	Japan Information Security Audit Association
JIS	Japanese Industrial Standard
METI	Ministry of Economy, Trade and Industry (Japan)
MIC	Ministry of Internal Affairs and Communications (Japan)
MISS	Minimum Information Security Standards (South Africa)
MOU	Memorandum of Understanding
NCPF	National Cybersecurity Policy Framework (South Africa)
NISC	National Center of Incident Readiness and Strategy for Cybersecurity (Japan)
NIST	National Institute of Standards and Technology (United States)
NCSC	National Cyber Security Centre (UK)
PaaS	Platform as a Service
PAIA	Promotion of Access to Information Act
RFQ	Request for Quote/Request for Quotations
SaaS	Software as a Service
SDGE	Smart Dubai Government Establishment
SITA	State Information Technology Agency (South Africa)
SOC	System and Organization Controls
UAE	United Arab Emirates



Executive Summary

With the technological advancements in cloud computing and the cost-efficiencies of cloud services, public cloud solutions offer numerous benefits for governmental operations.¹ Although countries acknowledge the benefits of cloud services for the public sector, the mainstream adoption in the public sector, especially in developing countries, is slow. Concerns for cybersecurity, data sovereignty, and privacy are impeding progress. These risks can be managed through appropriate institutional and procurement arrangements. However, many countries struggle with *how* to establish institutional mechanisms to procure cloud services from commercial providers in a secure and cost-efficient way. Responding to this need, **the World Bank's GovTech team has prepared this Note to provide institutional and procurement guidance and risk-mitigation methodologies for integrating cloud services into the public sector. The intended audience for this report includes World Bank client countries, practitioners, and multilateral and bilateral development partners.** The report aims to inform the audience about the range of institutional and procurement considerations when developing policies to preapprove and procure public cloud solutions.

A case study approach has been adopted to present the experiences of four countries and one city – Australia, Japan, South Africa, the United Kingdom (UK), and the city of Dubai, United Arab Emirates (UAE) – that have taken various paths to develop institutional coordination mechanisms and procurement arrangements for public sector cloud service procurements. The strength of these case studies is in their diversity; they not only represent different geographic regions, but also offer variation in their cloud procurement approaches. Their deep experiences in the cloud security and procurement realms also offer readers a wealth of good practices to consider when developing their own cloud security and procurement policies. The majority of the case studies are advanced digital governments. Their experiences can offer good practices for readers to consider and implement when adopting public cloud solutions.

Developing countries face unique challenges in adopting public cloud solutions that must also be considered. As such, the South Africa case study is intended to offer additional recommendations for developing countries. A comparative analysis is therefore conducted to identify lessons learned across the five case studies grouped into three key thematic areas: (1) Institutional Coordination Mechanisms; (2) Data Classification and Security Framework; and (3) Procurement Arrangements. The report highlights several similarities and variations across the five case studies, as described in Table 1 below.

TABLE ES.1 - Major Similarities and Variations in Case Studies




	 Pillar 1: Institutional Coordination Mechanisms	 Pillar 2: Data Classification and Security Framework	 Pillar 3: Procurement Arrangements
Similarities	<p>Cloud-First Policy: Each case study has adopted a “cloud first” principle within its government digital services policy. Under this principle, public sector organizations – referred to in this report as “procuring agencies” – must first consider and fully evaluate potential cloud solutions before considering any other option. Cloud first concepts may also promote consideration of public cloud services before other types of cloud deployment.</p> <p>The cloud first principle is typically articulated within top-level government policies and strategies that promote government cloud adoption. Such policies aim to integrate key digital service agencies, procurement specialists, and cybersecurity agencies into the government-wide cloud adoption approach.</p>	<p>International certification: The report underscores similarities in the use of international certifications within the case studies’ security frameworks. For example, Japan and Dubai leverage International Standards Organization (ISO)/International Electrotechnical Commission (IEC) certifications as part of their preapproval processes, while others view ISO/IEC certifications as beneficial but not required.</p> <p>Preapproval: Most of the case studies have established cybersecurity agencies or cloud procurement offices, tasked to assess and preapprove Cloud Service Providers (CSPs) for hosting government data. The preapproval process involves verification that the CSPs comply with a government’s cybersecurity requirements issued through a standard, manual, guidance, or cybersecurity framework.</p> <p>Continuous security monitoring: This report also highlights some similarities in security monitoring processes. For example, all case studies require procuring agencies to conduct continuous security monitoring of their cloud services through the entire procurement lifecycle. Similarly, most case studies require periodic reassessments of CSPs and their cloud services. Moreover,</p>	<p>Vendor Lock-in and Payments: Most of the case studies address the issues of vendor lock-in and transparency in payment methods.</p>

Table ES.1 continued







	 Pillar 1: Institutional Coordination Mechanisms	 Pillar 2: Data Classification and Security Framework	 Pillar 3: Procurement Arrangements
		most case studies emphasize the responsibility of each procuring agency to understand its own security needs during the cloud procurement lifecycle.	
Variations	<p>Institutional Framework: Japan has established a “Centralized” model wherein a single bureaucratic entity facilitates the cybersecurity assessment of cloud services and offers a list of preapproved cloud services to be procured by public sector entities.</p> <p>South Africa’s “Decentralized” model provides guidance to procuring agencies on various considerations, including cybersecurity needs, for each agency’s cloud procurement activities.</p> <p>Australia, Japan, and the UK have adopted a “Hybrid” model wherein multiple government entities share the responsibilities for preapproval and procurement.</p>	<p>Data Classification: Most case studies have tiered data classification systems based upon Confidentiality, Integrity, and Availability (CIA) requirements. In contrast, Japan only includes one data classification level in its cloud procurement approach.</p> <p>International Standards versus Internal Controls: Some models – for example, Japan and Dubai – base their security controls upon other international cybersecurity standards such as the <i>ISO/IEC 27000</i> family of controls. In contrast, Australia uses standards developed by the U.S. Government’s National Institute of Standards and Technology (NIST). Others, such as South Africa and the UK, do not mandate alignment with any specific security standards or certifications for cloud procurements.²</p> <p>Data Residency Approaches: South Africa and Dubai have legal requirements limiting the type of data that can cross national borders. In contrast, Australia, Japan, and the UK require each procuring agency</p>	<p>Marketplaces versus Preapproved Lists: Australia, the UK, and Dubai have marketplaces to promote simple, standardized procurements of cloud services. Japan, on the other hand, has a preapproved cloud services list (“ISMAP Cloud Service List”) from which procuring agencies can conduct procurements. The specific contracting method depends on characteristics of each agency and project. South Africa presently does not offer a marketplace or preapproved listing of cloud services.</p>

Table ES.1 continued

	 Pillar 1: Institutional Coordination Mechanisms	 Pillar 2: Data Classification and Security Framework	 Pillar 3: Procurement Arrangements
		<p>to make risk-informed decisions on data residency for certain data classification levels.</p> <p>Third-Party Assessments versus Internal Assessments: Australia, Japan, and Dubai have established third-party assessment (3PA) mechanisms to promote standardized assessments of cloud services</p>	

In all case studies, each procuring agency is ultimately responsible for determining the classification levels for its data and buying a cloud service that satisfies its security and business requirements.

Key Decision. *This report offers some key takeaways based upon some “good practices” observed in the case studies. These takeaways aim to provide client countries with a clear, simplified approach to institutional coordination mechanisms and procurement arrangements for public sector cloud service procurements. Further, this report suggests good practices under the three pillars for governments looking to securely integrate public cloud solutions into their government operations.*



Pillar 1: Institutional Coordination Mechanisms

- **Cloud First Principles and Top-Level Policy Guidance:** Establishing a government-wide “cloud first” principle and a whole-of-government approach to cloud procurements can help to promote a standardized process for preapproving CSPs and their cloud services.
- **Institutional Framework:** Considerations may include designating a central cybersecurity body to facilitate the preapproval or certification of CSPs and their cloud

services and a cloud procurement office (CPO) to facilitate the procurement of cloud services through a cloud marketplace. Some countries may have the capacity to establish new offices, while other countries may designate existing offices or working groups to address CSP preapproval and procurement policies.



Pillar 2: Data Classification and Security Framework

- **Data Classification Framework:** Most countries already have a government-wide data classification scheme based upon CIA requirements. The data classification schemes typically include both government data and any personal data of its citizens – personally identifiable information, or PII – that it handles. The World Bank’s *Data Classification Matrix and Cloud Assessment Framework* provides a suggested framework for how to align data classification schemes with key issues such as the type of systems to be procured – for example, on-premises computing versus public cloud – data residency requirements, and preapproval activities. Procuring agencies may consider this scheme, in coordination with their respective government’s data classification approach, to help determine how to handle data within public cloud environments.

- **Data Residency:** Data residency requirements for cloud services handling certain data classification levels such as Official, Secret, or Top Secret are also of major importance. Cloud services handling data below these thresholds do not require data residency requirements (see *Data Classification Matrix and Cloud Assessment Framework*).
- Another key consideration is the domestic legal requirements of CSPs. Risk-informed decisions on adopting public cloud services could include conversations with CSPs to understand their legal obligations for their national governments, especially for sensitive data of citizens such as personally identifiable information (PII).
- **Security Controls Based upon International Standards:** There are various approaches to establishing security controls for the preapproval of CSPs.
 - For example, a country could consider leveraging *existing* international cybersecurity standards, such as ISO/IEC and Cloud Security Alliance (CSA) security controls. Both ISO/IEC and CSA certifications are highly respected, widely used global cybersecurity standards that many CSPs already possess. Moreover, it is much simpler and easier for countries to verify a CSP's compliance with these international certifications instead of developing their own set of security controls. In addition, the adoption of international certifications could help harmonize security assessments across countries.
 - Countries may also consider a more advanced, *tiered* security framework corresponding to the classification level of the data to be handled by a CSP, akin to the US government's FedRAMP system. This type of security control framework is a possibility for more advanced countries.
- **Security Assessments:** Countries are encouraged to facilitate a standardized approach whereby CSPs are preapproved by a government agency, an accredited third-party assessor (3PA), the cybersecurity agency, or a combination thereof to handle certain government data. Such reviews could also benefit from the concept of "inheritance," whereby every layer of the cloud stack is certified. This means that if a Software as a Service (SaaS) system is built upon a certified Platform as a Service (PaaS) or Infrastructure as a Service (IaaS), an assessor only assesses the SaaS.
- **Local CSPs vs Hyperscalers:** Using standardized security framework and associated requirements, governments could help to promote local CSPs identified as small and medium-sized enterprises (SMEs) that need information on government's security requirements to register as eligible providers. Hyperscalers generally have already implemented international security standards, which gives them an edge over local SMEs in terms of government contracts.
- **Continuous Monitoring:** Procuring agencies are ultimately accountable for the security of their IT enterprises. They are responsible for working with CSPs and other stakeholders such as 3PAs to maintain a secure public cloud environment. To this end, continuous monitoring activities may include security incident notifications, re-verifications at least every two years, and security control change notifications.



Pillar 3: Procurement Arrangements

- **Centralized Marketplace for Cloud Services:** An online marketplace of CSPs and their cloud solutions for procuring agencies may be considered. Typically, to be added onto a marketplace, a CSP would be expected to sign a general "Cloud Framework Agreement" that includes basic cybersecurity and data privacy provisions such as compliance with relevant national laws that can be verified by the country. The Cloud Framework Agreement would require periodic updates, based upon the limits of the relevant procurement legislation for framework agreements in countries. A marketplace typically includes pricing for each cloud service offering and clearly identifies a CSP's preapproved status. Alternatively, countries may instead choose to establish a preapproved listing of CSPs and their cloud services that is easily accessible to procuring agencies.
- Countries may also consider setting up framework agreements—"master agreements"—with hyperscalers to facilitate streamlined and low-cost purchases of basic cloud services such as cloud storage and hosting for multiple procuring agencies. These setups would allow procuring agencies to directly purchase these basic services from hyperscalers, as opposed to buying these services through resellers on a marketplace or preapproved list.

- **Selecting a Cloud Offering:** Cloud offerings may be reviewed by procuring agencies on the marketplace or the preapproved list to determine which CSPs meets its specific business and security requirements. There are numerous ways to begin procurement of a cloud service once selected. For example, a procuring agency may issue a tender or RFQ to facilitate competitive bidding between CSPs on the marketplace. A procuring agency may also consider choosing a cloud service based upon a “best value” standard that considers cost, security, total cost of ownership, and other relevant considerations.
- **Simplified and Standardized Contracts:** Simple and standardized contracts are a preferred method for procuring cloud services. Box 3.4 provides a standardized “Call-Off Contract” template for contracting with CSPs on a marketplace. For more complex solutions with specific functional requirements not available on the marketplace, procuring agencies may need to undergo Tenders or RFQs outside the marketplace to conduct functional evaluations of specialized cloud services not available on the marketplace.
- **Avoiding Vendor Lock-In:** Short-term contracts – for example, a two-year contract with limited annual renewals – help manage the risk of vendor lock-in. Procuring agencies should also be aware of portability fees, the

cost of transferring data from one CSP to another, before signing a contract. Procuring agencies may consider listing cloud portability tools and associated migration activities as optional services in the Tenders or RFQs to help them more easily migrate between CSPs.

- **Payment Methods:** Key considerations for countries seeking fair cloud prices include promoting CSP pricing transparency, allowing cloud service prices to fluctuate based upon market prices (enabling price reductions), allowing CSPs to offer different pricing models, and creating an on-demand, pay-as-you-go payment option to foster cost reductions.

Countries may wish to adopt the above recommendations to manage the risks of procuring public cloud services. These commercial offerings can be employed in tandem with other cloud deployment models – such as GovClouds – to facilitate a trusted Hybrid Cloud environment for governments. See also Box 3.3 for more information on interoperating different cloud environments through Open Application Programming Interface (Open API).

Appendix 1 provides a Step-by-Step Guide for countries to consider when beginning the cloud journey process for the public sector.



Introduction

Despite widespread awareness on the benefits of cloud computing, authorities in most of the World Bank's client countries have not explored the opportunity of adopting cloud computing solutions. Task teams are finding it difficult to provide relevant advice to the counterparts and address their concerns. Most authorities have identified risks of moving to cloud computing: Will their data be safe? Will they have sovereign control over access to data stored offshore? Will privacy be protected? These risks are real. Due to an inadequate assessment framework to identify and assess these risks, the typical response of most client governments is to develop a government's cloud (G-Cloud or GovCloud). This seems logical for more sensitive or mission-critical data. However, this is not enough. Adopting a hybrid cloud model, which leverages the cloud services from the private sector to work in conjunction with the G-Cloud can offer immense opportunities to save costs, improve security, enhance performance, and strengthen resilience in a post COVID-19 world. However, client governments need guidance to change their policy response on cloud computing - from the risk-avoidance to the one of risk-management.

This Note provides guidance on institutional and procurement arrangements and risk-mitigation methodology for acquiring and managing public cloud solutions using a whole-of-government approach.

A quick summary of cloud service models, cloud deployment models and 'Cloud-First' principle will help to contextualize the discussion on the main guidance.

1.1 Cloud Service Models

The US government's National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources – for example, networks, servers, storage, applications, and services – that can be rapidly provisioned and released with minimal management effort or service provider interaction.” NIST assigns five essential characteristics of cloud computing: on-demand self-service; broad network access; resource pooling; rapid elasticity; and measured service.³

The term, cloud services refers to a broad range of services offerings, which can be categorized as either Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS).

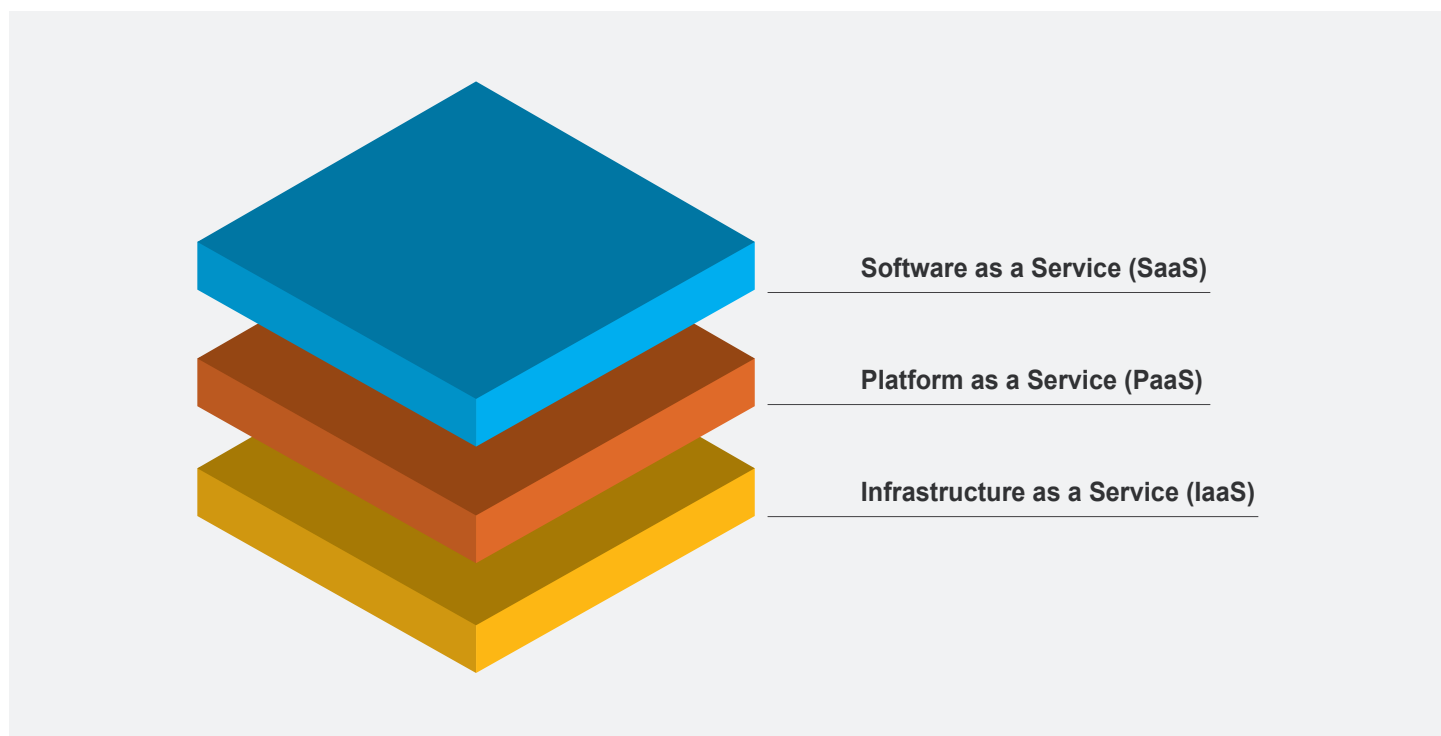
- **SaaS** is the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (web-based email), or a program interface. The consumer 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.⁴

- **PaaS** is the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. 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.⁵
- **IaaS** is the capability provided to the consumer 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 – for example, host firewalls.⁶

> > >

FIGURE 1.1 - Cloud Service Models

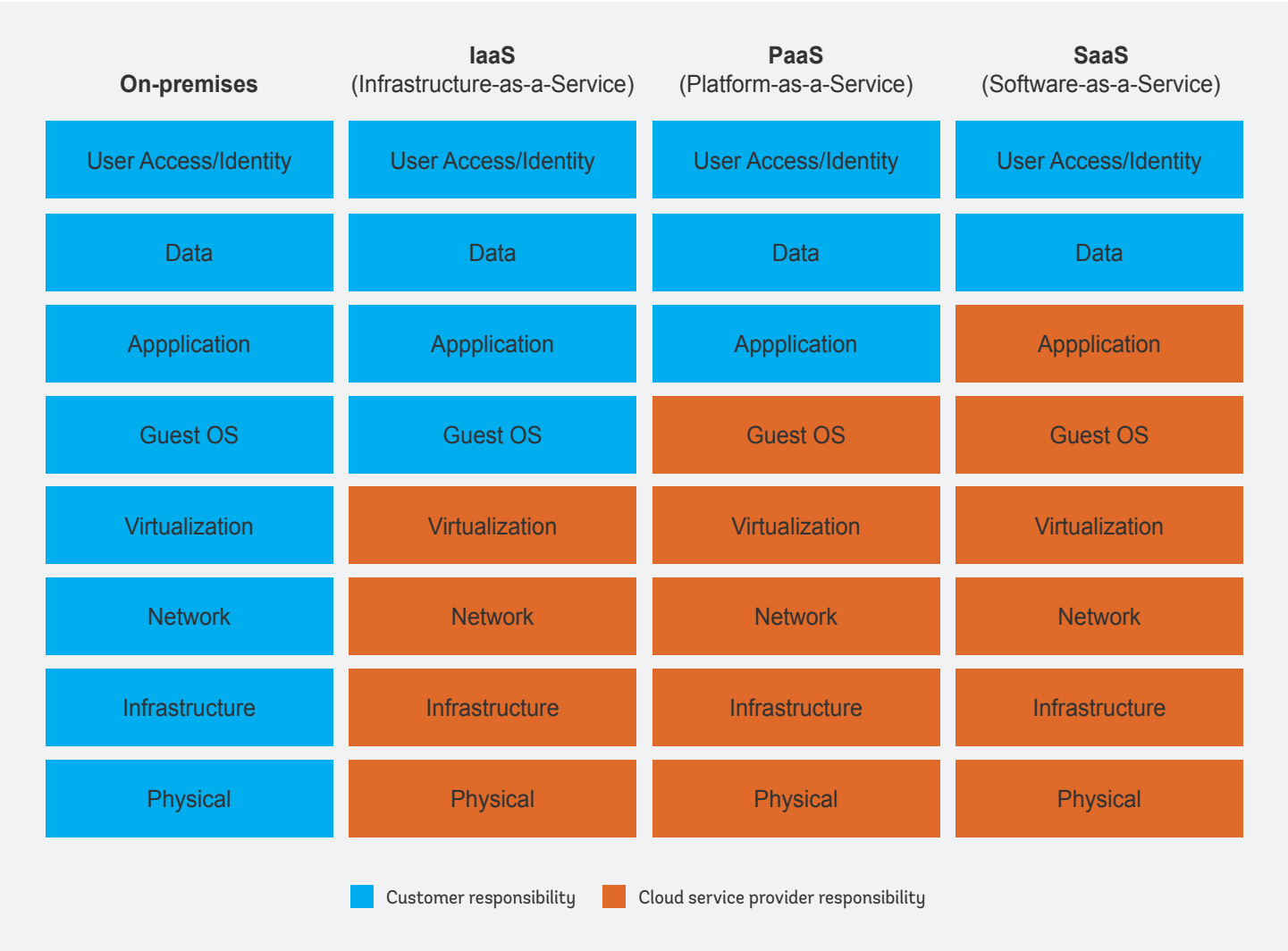


Source: [Cloud Information Center, gsa.gov](https://cloudinfo.gsa.gov/).

The top layer of a cloud service, the SaaS, is the most “packaged” solution that can be deployed by a CSP with minimal management requirements for a consumer. Going down the cloud service layers, PaaS and IaaS necessitate greater management and configurability requirements for the consumer. **Generally, customers have higher risk of vendor lock-in⁷ when more of the service is managed by the CSP.** As such, SaaS solutions have higher risk of vendor lock-in compared to PaaS and IaaS, as these two services are almost exclusively managed and configured by the CSP.

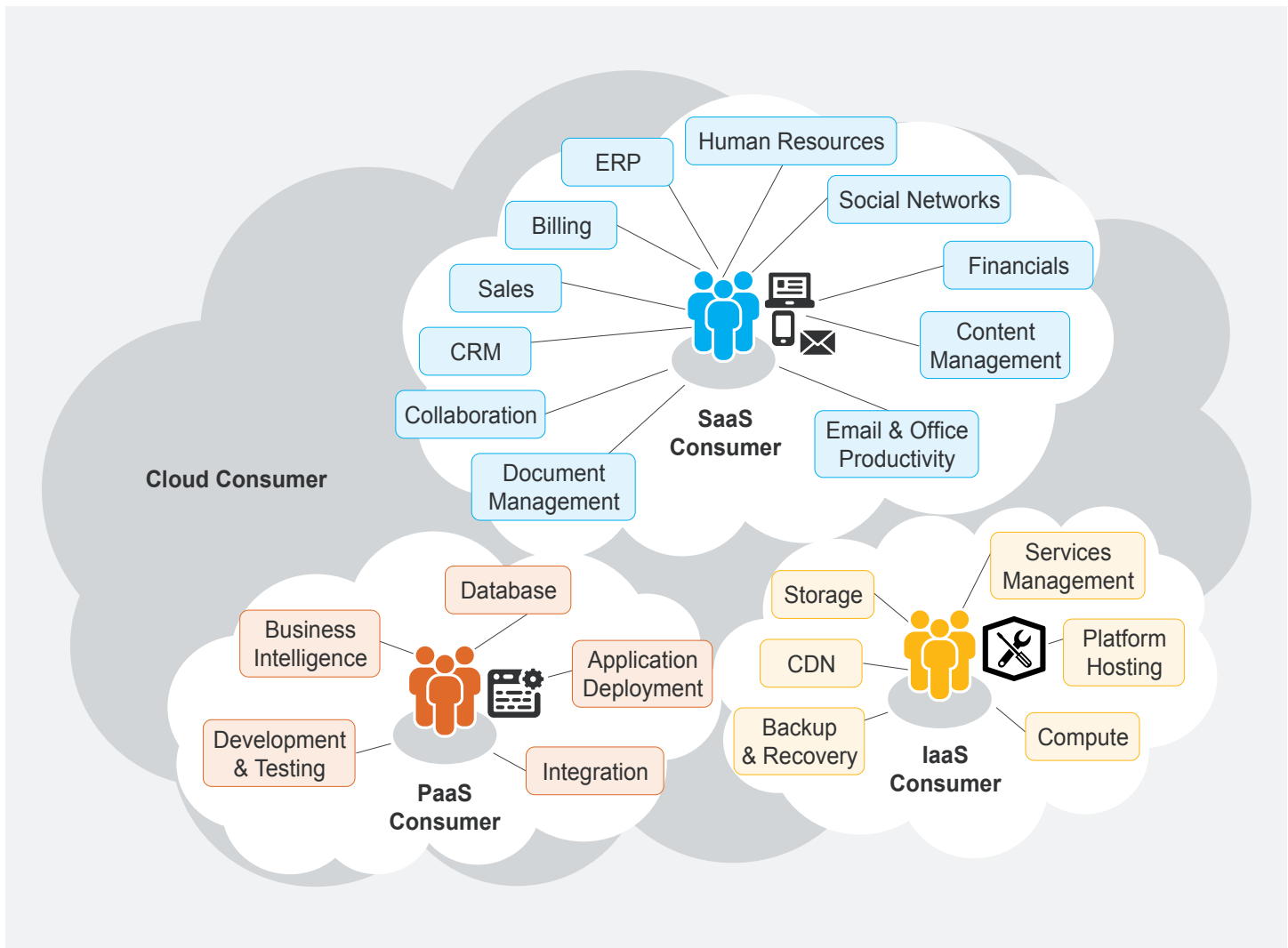
From a security perspective, each cloud service model requires a unique shared responsibility relationship between the consumer and the CSP. Compared to on-premises computing, where the consumer is predominately responsible for all aspects of security, cloud services assign some of the security responsibilities to the CSP. In general, the CSP security responsibilities of the consumer decreases as the cloud service model moves from IaaS to PaaS to SaaS, as shown below in Figure 1.2.

> > >
FIGURE 1.2 - Shared Responsibility between Consumer and CSP



Source: [Oracle Cloud Threat Report - Demystifying the Cloud Shared Responsibility Security Model](#).

Overall, the different cloud service models create a trade-off for government cloud consumers. SaaS solutions reduce the security responsibility burdens for the consumer but increase the risk of vendor lock-in. Conversely, PaaS and IaaS increase the security responsibility burdens for the consumer while decreasing the vendor lock-in risk. As Figure 1.3 below illustrates, each cloud service model can offer a range of digital tools for use by procuring agencies.

FIGURE 1.3 - Example Services Available to a Cloud Consumer (NIST SP 500-292)

Source: NIST.

1.2 Cloud Deployment Models

There are four cloud deployment models available to governments, as shown below in Figure 1.4:

1. **Private cloud** is provisioned for exclusive use by a single organization comprising multiple consumers. It may be owned, managed, and operated by the organization, a third party, or some combination, and it may exist on or off premises.⁸
2. **Community cloud** is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (such as government agencies). 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.⁹ A Government Cloud (GovCloud or G-Cloud) that hosts a government-wide data center shared by all government ministries is an example of a community cloud. G-Cloud examples include DubaiPulse and GOV.UK PaaS.

3. **Public cloud** 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

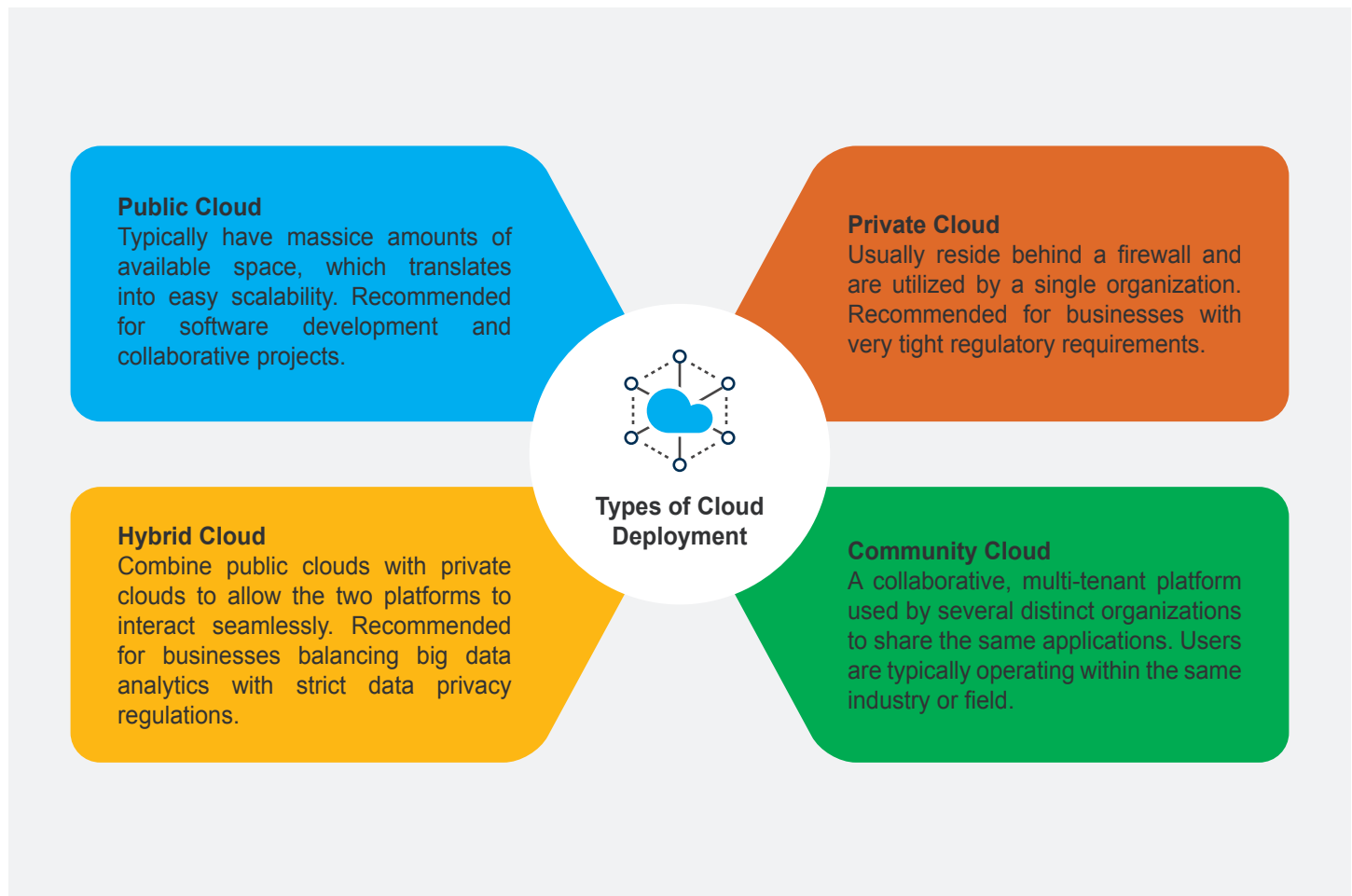
the cloud provider.¹⁰ Examples of public cloud providers include Microsoft Azure, Amazon Web Services (AWS), and Google Cloud.

4. **Hybrid cloud** is composed 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 processing and application.¹¹ For example, in some hybrid cloud environments, organizations connect a private cloud system such as payroll software with a public cloud for workload processing, while the data remains on-premises.

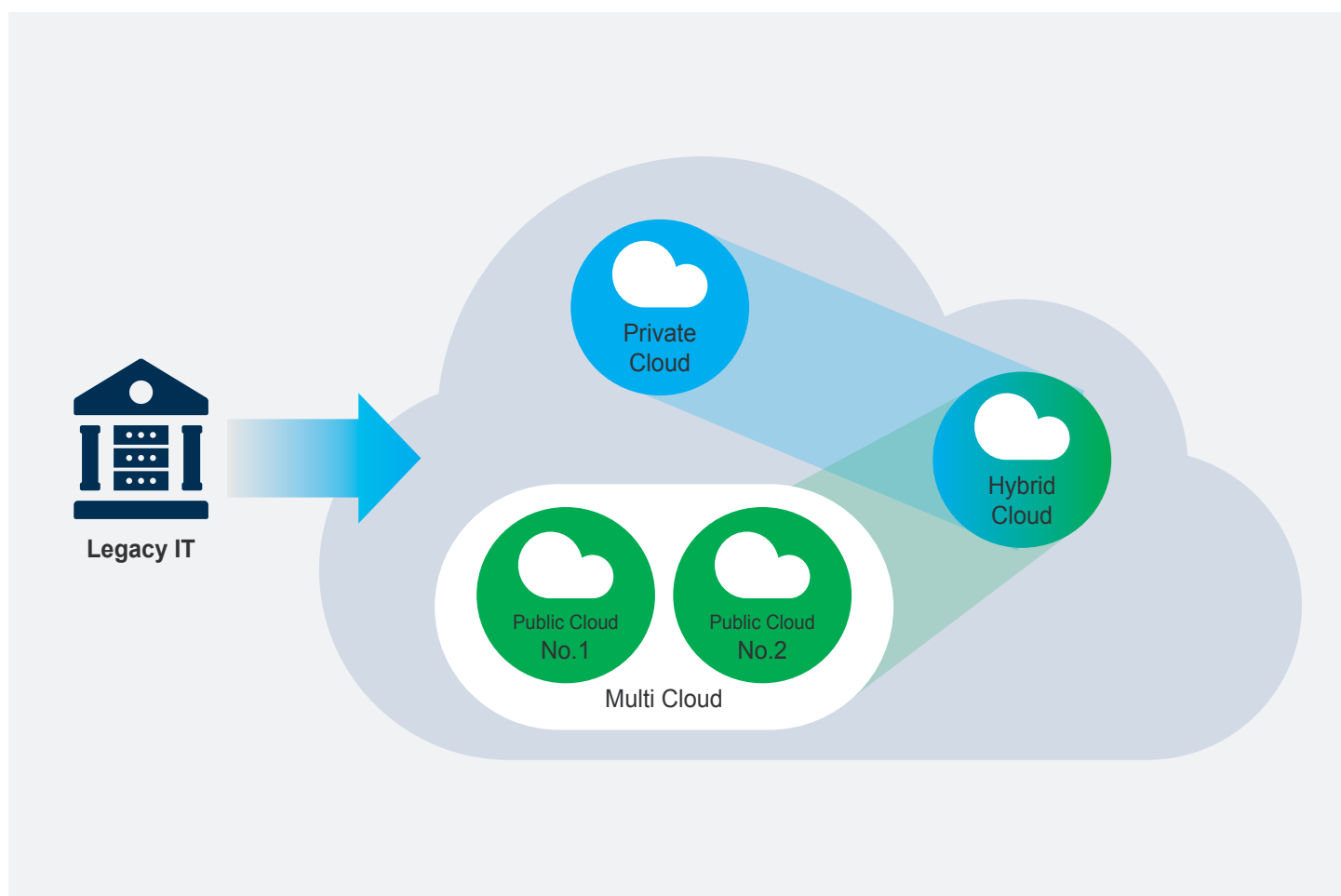
> > >

FIGURE 1.4 - Types of Cloud Deployment



Source: [4 Cloud Deployment Models: Their advantages and disadvantages - TurningCloud Solutions Blogs](#)

A procuring agency may choose a variety of cloud deployments to fit its needs. For example, a procuring agency may leverage public clouds for certain solutions, while leveraging private and hybrid clouds for other digital solutions. Figure 1.5 below is a visual depiction of a transition from legacy to a cloud environment.

FIGURE 1.5 - Different Cloud Deployment Schemes¹²

Source: World Bank.

Governments must also consider institutional frameworks and procurement processes to manage the potential risks of adopting cloud services. Procurement of public cloud services introduces new security considerations for procuring agencies that have traditionally relied upon on-premises computing services. CSPs assume much of the cybersecurity

and data privacy risks that were traditionally addressed by procuring agencies. As such, governments have created new institutional frameworks and pre-procurement certification processes to ensure cybersecurity risks are properly managed within these new public cloud arrangements.

1.3 Cloud Security Accreditations and Certifications

CSPs may also demonstrate their cybersecurity credentials through an accredited certification body—also called a third-party assessor. Some key terms for this process include the following.

- **Accreditation** is the formal recognition by an independent body, generally known as an accreditation body, that an individual or organization operates according to international standards.¹³ In terms of cloud security, an organization must receive an accreditation to become an accredited certification body capable of performing a conformity assessment of the security posture of a CSP and/or its cloud service offerings (CSOs).¹⁴
- **Certification** is the provision by an independent body of written assurance, such as a certificate, that the product, service, or system in question meets specific requirements.¹⁵ In terms of cloud security, a certification demonstrates that a cloud product, service, system, process, or CSP conforms to specified requirements such as international standards, as confirmed by an accredited certification body. Examples of cloud security certifications include ISO/IEC 27001, Cloud Security Alliance (CSA) Level 2 STAR, and Systems & Organizational Control 2 (SOC 2).
- **Conformity Assessment Activity** is the demonstration that specified requirements relating to a product, process, system, person, or body are fulfilled.¹⁶ In terms of cloud security, an accredited certification body may perform a “conformity assessment activity,” which includes a number of security tests, for a CSP and/or its CSOs to certify compliance with a standard such as ISO/IEC 27001.

1.4 Report Objective

The objective of this report is to assist readers in considering a framework for the preapproval and procurement of cloud services. This framework should ensure that national governments have the bureaucratic tools as well as the pre-procurement, procurement, and post-procurement processes in place to ensure sufficient cyber risk management of public cloud solutions for government agencies.

The report is structured as follows:

- Chapter 2 reviews lessons learned from the institutional coordination mechanisms and preapproval and procurement arrangements of the five case studies.
- Chapter 3 offers key takeaways and guidance moving forward for countries seeking to better leverage public cloud solutions.
- Annexes 1-5 provide case studies on the institutional coordination mechanisms and preapproval and procurement arrangements of four national governments and one city (Australia, Japan, South Africa, UK, and the city of Dubai, UAE).

The findings of this report facilitated the development of the World Bank’s *Data Classification Matrix and Cloud Assessment Framework* for the preapproval of public cloud services that will serve as a reference model for countries, particularly developing countries, as they transition to cloud first postures.



Lessons Learned: A Comparative Analysis of Case Studies

The experiences captured in the five case studies provide insights into good practices for institutional coordination mechanisms and procurement arrangements for integrating cloud services into public entity operations. Each case study presents various policies and processes that can be helpful for World Bank clients and donors/partners to consider when promoting their own cloud security and procurement practices.

Table 2.1 below offers a benchmarking of the five case studies against three relevant indices: the World Bank's GovTech Maturity Index (GTMI), the UN's E-Government Development Index (EGDI), and the MIT Technology Review's Global Cloud Ecosystem Index. As presented below, Australia, Japan, the UK, and the UAE are advanced in all three indices, whereas South Africa has a lower rating.

TABLE 2.1 - Benchmarking the Case Studies using the GTMI (updated October 2022), the EGDl (updated 2022), and the Global Cloud Ecosystem Index (updated 2022)

Case study	GMTI (from 0 to 1)	EGDI (from 0 to 1) ¹⁸	Global Cloud Ecosystem Index (from 0 to 10) ¹⁹
Japan	0.767	0.9002	7.8
Australia	0.811	0.9405	7.9
UK	0.840	0.9138	8
South Africa	0.562	0.7357	6
UAE*	0.961	0.9010	7.3

Note: *This table refers to UAE, as Dubai is not a country and thus not included in the GTMI.

Below is a discussion on key similarities and differences between these case studies, divided into three pillars:

- Pillar 1: Institutional Coordination Mechanisms
- Pillar 2: Data Classification and Security Framework
- Pillar 3: Procurement Arrangements

2.1 Institutional Coordination Mechanisms

This section provides a discussion of similarities and differences, along with a discussion on the strengths and weaknesses, of the institutional coordination mechanisms for procuring secure cloud services.

2.1.1 Cloud First Principle

Each case study has adopted a cloud first principle within its government digital services policy. Under this principle, procuring agencies are required to first consider potential cloud solutions before considering any other option, such as on-premises computing solutions. Many countries also require procuring agencies to consider public cloud solutions before any other cloud deployment model if that public cloud provides appropriate security controls for the data to be handled.

In four of the five case studies, cloud first principles are articulated within top-level government policies

and strategies that pertain to the whole-of-government. For example:

- The Australian government's original cloud security guidance, the *Australian Government Cloud Computing Policy* (2014),²⁰ created a cloud first mandate for its procuring agencies. Its updated policy, the *Secure Cloud Strategy* (2019),²¹ also retains the cloud first policy.
- The Japanese government's *Cloud Adoption Policy for Government Information Systems* (2018) maintains a cloud first principle that was previously articulated by past policies.²²
- The UK government's *Cloud First Policy* (2013) promotes the cloud first principle.²³
- The Dubai Government Excellence Program (DGEP) published a key performance indicator (KPI) for public agencies to abide by the cloud first principle.²⁴

South Africa has not yet finalized its top-level policy on cloud computing. Its *National Policy on Data and Cloud* remains in draft form. However, in its current draft form, the National Policy does not articulate a cloud first principle. But a February 2022 *Public Service Cloud Computing Determination and Directive* issued by South Africa's Department of Public Service and Administration (DPSA) establishes a cloud first principle for public sector organizations.²⁵



2.1.2 Top-Level Policies and Strategies

The five case studies have top-level policy guidance to promote consistency of government approach toward cloud procurements.

- Australia's *Secure Cloud Strategy* underpins the government's approach toward cloud preapproval and procurement. The Strategy also integrates various other government cybersecurity guidance documents to inform procuring agencies working to follow the Strategy's guidance.
- Japan's *Cloud Adoption Policy for Government Information Systems* informs its centralized approach toward cloud procurements, the Information System Security Management and Assessment Program (ISMAP).
- The South African government is deliberating on the finalization of its draft *National Data and Cloud Policy* published in April 2021 by the Department of Communications and Digital Technologies (DCDT).²⁶
- The UK's *Cloud First Policy* drives many of the government's initiatives and strategies to promote secure acquisition of cloud solutions across public organizations, including the G-Cloud Framework and Digital Marketplace.
- The Dubai Digital Agency (DDA) develops and oversees its policies and strategies to promote Dubai's digital transformation.

These top-level policies, and supporting cybersecurity guidance and initiatives, represent an important first step for countries beginning the cloud procurement journey. The top-down policy approach encourages consistent implementation of preapproval and procurement processes by public organizations seeking to procure public cloud solutions. Moreover, as detailed below, the use of standardized frameworks and processes can also allow for streamlining of CSP and cloud service approvals across procuring agencies.

2.1.3 Institutional Framework

While the case studies have strong similarities in declaring cloud first principles and developing top-level cloud procurement policies and strategies, **they have major differences in the institutional frameworks to advance cloud preapproval and procurement.** These differences can be categorized into three models: Centralized, Decentralized, and Hybrid. Table 2.2 below summarizes the strengths and weaknesses of each model.

Centralized Model: Japan uses a centralized approach that puts the responsibility upon ISMAP, in collaboration with third-party assessors, to preapprove cloud services that are then added to its Cloud Service List. In turn, procuring agencies may issue tenders for cloud services on the Cloud Services List, without the need to conduct their own security assessment of the cloud service.

Decentralized Model: South Africa promotes a more decentralized approach. The *Public Service Cloud Computing Determination and Directive* issued by the Department of

Public Service and Administration's (DPSA) offers guidance on how procuring agencies should approach the cloud service procurement process, including business and security aspects of cloud procurement. Procuring agencies are responsible for finding, assessing and approving, and procuring cloud services.

Hybrid Model: In this model adopted by Australia, the UK, and Dubai, various government entities share the preapproval and procurement responsibilities. Unlike in Japan, multiple government entities help to facilitate the preapproval and procurement of CSPs and their cloud solutions. And unlike in South Africa, procuring agencies receive support from procurement offices in finding and assessing cloud services. Under the Hybrid approach, each procuring agency is ultimately responsible for assessing the security of cloud services against its own security needs, sometimes with the assistance of third-party assessors.

In the UK, the Crown Commercial Service's (CCS) Digital Marketplace offers a range of cloud solutions along with

information on relevant security certifications, pricing, functional offerings, among other information. Agencies procuring cloud services off the Digital Marketplace are responsible for their own security assessments and approvals.

In Australia, cloud service offerings can be assessed and preapproved under the Australian Cyber Security Centre's (ACSC) Infosec Register Assessors Program (IRAP). In turn, the Digital Transformation Agency's (DTA) Cloud Marketplace offers a range of cloud solutions, including offerings from IRAP-assessed CSPs and CSPs without an IRAP assessment.

In Dubai, the Dubai Electronic Security Center (DESC) oversees the certification audits of CSPs conducted by third-party Certification Bodies under the *CSP Security Standard*. In turn, procuring agencies may purchase the cloud services of CSPs with or without certification on Dubai's eSupply portal, depending on the data type and the risk assessment process of the entities involved.

> > >

TABLE 2.2 - Summary of Institutional Frameworks of the Case Studies

Case study	Model	Strengths	Weaknesses
Japan	Centralized	<ul style="list-style-type: none"> Streamlines security responsibilities within one organization, facilitating the preapproval of cloud services and listing the preapproved cloud services. Eases the security assessment process for procuring agencies. 	<ul style="list-style-type: none"> Available preapproved cloud offerings may be limited compared to other models. Centralized system could create bottlenecks.
South Africa	Decentralized	<ul style="list-style-type: none"> Standardized procurement guidance provides for flexibility in agency-level cloud assessment and approval process. Empowers agencies to tailor their assessment, approval, and procurement activities to its unique circumstances. 	<ul style="list-style-type: none"> Available preapproved cloud offerings may be limited compared to other models. Centralized system could create bottlenecks.
Australia	Hybrid	<ul style="list-style-type: none"> Streamlines security responsibilities within one organization approving or verifying the certification of cloud services. Centralized marketplace eases the process of selecting and assessing various cloud services. 	<ul style="list-style-type: none"> Multiple organizations with varied responsibilities could cause complexity and confusion.
UK			
Dubai			

2.2 Data Classification and Security Framework

This section discusses the similarities and differences among the case studies, along with a discussion on the strengths and weaknesses, of the data classification and security framework considerations for secure cloud services.

2.2.1 Data Classification

Each case study has its own, unique data classification system. That said, there are some commonalities among many of the data classification systems. For example,

many case studies use the Confidentiality, Integrity, and Availability (CIA) framework when considering levels of injury in case of a security incident. Many countries also aim to distinguish between lower-priority “Sensitive” or “Protected” data versus higher-priority “Classified” or “Secret” data. Japan is unique in that the ISMAP system only pertains to one data classification level – “Confidential 2,” which corresponds with the US government’s FedRAMP Moderate Impact Level.

> > >

FIGURE 2.1 - Comparison of Data Classification Levels

Japan (ISMAP)	Australia	UK	South Africa	Dubai
<ul style="list-style-type: none">Confidential 2	<ul style="list-style-type: none">Unclassified (Unofficial, Official, Official: Sensitive)Classified (Protected, Secret, Top Secret)	<ul style="list-style-type: none">OfficialSecretTop Secret	<ul style="list-style-type: none">RestrictedConfidentialSecretTop Secret	<ul style="list-style-type: none">OpenShared-confidentialShared-sensitiveShared-secret

The case studies limit the types of data that a public cloud may handle. For example:

- Japan’s ISMAP only approves public cloud services for the handling of data at the Confidential 2 level.
- The Australian government allows CSPs *without* security clearances to handle data at or below the Official: Sensitive level. CSPs that handle data classified at the Protected level and above are required to have personnel who hold security clearances at the commensurate level.
- The UK government does not have any official limitation on the types of data to be handled by public clouds. However,

the vast majority of UK government data is marked Official and agencies may make case-by-case determinations if a public cloud service provider may handle such data.

- South Africa’s *Determination and Directive* stipulates that agencies must, as far as practically possible, avoid moving data classified as Secret or Top Secret to public clouds.
- Dubai requires procuring agencies to purchase the public cloud services of certified CSPs to handle any Shared data.

2.2.2 Data Residency Requirements

Cases study countries also vary in their data residency requirements (Figure 2.2). Only South Africa and Dubai have data residency requirements for data handled by public cloud service providers.

> > >

FIGURE 2.2 - Comparison of Case Studies' Data Residency Requirements

<p>Required</p>	<ul style="list-style-type: none"> • South Africa: Public cloud data must always reside within the borders of South Africa, with limited exceptions. • Dubai: Dubai forbids the handling of Shared data outside the UAE. In addition, CSPs handling Shared data for government entities must have a minimum of two data centers within the country's geographic jurisdiction. However, there is an exemption process for procuring agencies seeking to host shared data outside UAE, which is based on a risk assessment process
<p>Recommended</p>	<ul style="list-style-type: none"> • Australia: Recommends cloud consumers use CSPs and cloud services located in Australia for handling their sensitive and security-classified information. Australia also requires CSPs handling data at or above the Official:Sensitive data level to obtain a Hosting Certification Framework (HCF) certification. • UK: Recommends public agencies to consider the implications of where data is hosted. • Japan: Procuring agencies should strongly consider the potential risks of the handling of data that may become subject to foreign laws and regulations when selecting cloud service offerings.

2.2.3 Security Controls

Each case study has its own, unique regime of security controls for the preapproval of public cloud services.

Japan and Dubai developed their own control regimes based upon existing international standards. Australia bases its controls upon NIST standards. Other countries (e.g., UK and South Africa) rely more directly upon existing laws, regulations, and guidance.

- ISMAP uses *Japanese Industrial Standard (JIS)* controls,²⁷ based upon the ISO/IEC 27000 family of standards, as the criteria against which to evaluate the security of cloud services. ISMAP also maps the JIS standards to NIST Special Publication 800-53 (Rev. 4) and Japan's own domestic security control framework. Similarly,

Dubai's *CSP Security Standard* requires CSPs to obtain the following international certifications: ISO/IEC 27001 certification with the ISO/IEC 27017 extension and the CSA Level 2 STAR.

- Australia uses the *Information Security Manual (ISM)*²⁸ and its associated *Cloud Security Controls Matrix (CSCM)*²⁹ to evaluate the security of cloud services. The ISM draws the foundation of its framework from the NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Lifecycle Approach for Security and Privacy*.
- The UK government does not subscribe to one type of cybersecurity standard or set of security controls when assessing cloud services. Instead, it has several

security compliance requirements as part of the Digital Marketplace's G-Cloud Framework. The UK government also encourages CSPs to consider various baseline security guidance, especially the National Cyber Security Center's (NCSC) *14 Cloud Security Principles*.³⁰

- South Africa does not have a centralized set of security controls for cloud services procured by procuring agencies. Instead, it refers to existing national laws and agency-specific information security requirements.

Moreover, Australia and the UK state that any third-party certifications such as ISO/IEC certifications possessed by a CSP are taken under consideration during the security assessment process. However, such certifications are not required. In essence, they are seen as beneficial, but not mandatory.

2.2.4 Security Assessments

Each case study employs its own unique process for cloud preapproval to ensure procuring agencies properly assess

and mitigate risk before adopting public cloud services. Table 2.3 below reviews the various preapproval and procurement considerations and activities of each country.

- **Security Self-Assessment:** Are procuring agencies required to assess their own risk profiles before assessing cloud services?
- **Third-Party Assessors:** Do third-party assessors conduct a security assessment of the CSP as part of the review process?
- **Assessment Reuse:** Can CSPs share third-party assessments with multiple procuring agencies?
- **Controls Inheritance:** As part of the security assessment, do cloud services inherit the security controls of other cloud services they are built upon?
- **Reassessment Requirements:** Must approved CSPs and their cloud services be periodically re-assessed?

> > >

TABLE 2.3 - Comparison of Security Assessment Considerations and Activities

	Japan	Australia	UK	South Africa	Dubai
Security Self-Assessment	Yes	Yes ("Phase 2A" Report)	Yes	Yes	Yes
Third-Party Assessments	Yes ("ISMAP Assessors")	Yes ("IRAP Assessors")	No	No	Yes ("Certification Bodies")
Assessment Reuse	Yes (approved services added to Cloud Service List)	Yes	No	No	Yes
Controls Inheritance	No	Yes	Case-by-case	Case-by-case	Yes
Reassessment Requirements	Every 12 months	Every 24 months	24-month maximum G-Cloud Contract	Contracts cannot exceed 5 years	Basic reviews every 12 months and full recertifications every 3 years.

Some good practices from a review of the case studies' security assessments include:

- In general, **procuring agencies conduct a security self-assessment of their own systems** related to data classification levels, security requirements, business needs, and risk management considerations. This self-assessment helps align an agency's needs with the available cloud services.
- Australia, Japan, and Dubai use **third-party assessors (3PAs) that conduct standardized security assessments of CSPs**. This process allows agencies to assess cloud services and CSPs in comparison to each other using consistent, standardized assessment forms. The CSPs pay for the fees of the 3PA. The fee structure is established by the government through framework contracts with the approved 3PA.
- In Australia, **CSPs are encouraged to share IRAP assessments with other agencies**, thus streamlining approval processes for that CSP and its cloud services across the government.
- All countries require either mandatory reassessments or establish maximum contract lengths to help ensure ongoing reviews of a CSP's security posture.

2.2.5 Continuous Monitoring

All case studies require procuring agencies to work with CSPs and, in some cases, 3PAs to continuously monitor the security of a cloud service. For example, under Japan's ISMAP, cloud services must be renewed on an annual basis by ISMAP Assessors to ensure the continued security of each offering. Other countries similarly engage in long-term continuous monitoring through mandatory security reassessments, incident reporting requirements, and guidance for cloud lifecycle security.

2.3 Procurement Arrangements

This section provides a discussion of similarities and differences, along with a discussion on the strengths and weaknesses, of the arrangements to procure cloud services.

2.3.1 Finding and Selecting Cloud Services

Finding Cloud Services. Some case studies offer a centralized marketplace of cloud services. Australia, the UK,

and Dubai have developed online marketplaces for cloud services for procuring agencies.

For example, the UK's Digital Marketplace requires each CSP to sign the UK's G-Cloud Framework, a contractual agreement between the CSP and the UK government's CCS. The G-Cloud Framework requires suppliers to self-declare compliance with various cybersecurity and data privacy-related requirements.

- The UK's self-declaration model works well in a competitive, high-capability economy in which CSPs are held to high standards by both CCS and market competitors.
- In this system, there is little incentive to falsify self-declarations as failure to deliver services as advertised would likely result in the reduction or elimination of future government contracts. Procuring agencies could replace the CSP with a more suitable vendor.

Australia's Cloud Marketplace is a panel arrangement wherein CSPs are appointed to supply services for a set period of time under agreed terms and conditions. In contrast to the UK model, DTA releases periodically releases Request for Tender for CSPs to be added to the Cloud Marketplace. DTA must review and then approve these tenders—as opposed to the self-declaration model for the UK's Digital Marketplace.

Dubai's eSupply is the main online portal for suppliers, including CSPs, to participate in online bidding for government contracts. Any company may register as a supplier on eSupply. Procuring agencies may issue RFQs seeking cloud services from suppliers on eSupply. Another mechanism is a listing of preapproved cloud offerings. For example, Japan's ISMAP Cloud Services List provides procuring agencies with an updated list of preapproved cloud services. South Africa does not currently have a centralized List or Marketplace of cloud service offerings. Instead, each procuring agency conducts its own market research or Open Tender process to begin its cloud procurement activities.

Selecting and contracting with CSPs. Marketplaces are designed to facilitate simplified, short-term contracts for cloud services.

- In the UK, a procuring agency can issue a Call-Off Contract with a CSP for a commercial-off-the-shelf (COTS) cloud solution under the G-Cloud Framework on the Digital Marketplace. If only one supplier meets its requirements, it can directly issue the Call-Off Contract. If, on the other hand, there are several potential suppliers, a procuring agency may review and select a service based

upon the lowest-priced offering or a best value purchase based upon numerous factors, such as total cost of ownership, technical merit and functional fit, and service management. CCS provides a standard template Call-Off Contract for procuring agencies.

- In Australia, each procuring agency seeking a cloud service must undergo a competitive bidding process under an RFQ to achieve best value for money. Once a procuring agency selects its vendor, it forms a contract under the Cloud Marketplace panel arrangement. DTA provides a standardized contract templates for procuring agencies using the Cloud Marketplace.
- Under Dubai's eSupply, the specific procurement requirements for a cloud service under an RFQ varies depending on requirements for each project, for example, whether it handles Shared data and thus requires the CSP to be certified through the *CSP Security Standard*.

Security is a key consideration when selecting cloud services from the marketplaces. For example, the Australian marketplace notes whether its listed cloud services are IRAP-assessed. Moreover, the UK's Digital Marketplace also lists the cybersecurity certifications and standards for each CSP and its cloud services.

Another key consideration when selecting cloud services is cost, including total cost of ownership.³¹ Other

considerations may include business and operational needs, technical fit of the service, and service management. The UK's Digital Marketplace and Australia's Cloud Marketplace also include pricing information for cloud services. The marketplaces offer mostly COTS cloud solutions. In certain cases, procuring agencies with specific functional requirements that go beyond COTS offerings available on the marketplaces may issue a separate tender or RFQ off the marketplace for such specialized cloud services. For example, UK procuring agencies coordinate with the CCS to issue a Request for Tender for specialized cloud services.

The UK has also entered into separate agreements with hyperscaler providers such as AWS, IBM, and Microsoft, to allow streamlined and discounted cloud services for procuring agencies. These arrangements allow procuring agencies to purchase hyperscaler services such as cloud storage and compute directly from the hyperscalers through direct award or competitive bidding. For Japan, procuring agencies may contract with cloud services from its ISMAP Cloud Service List. The procuring agencies have flexibility in how to procure cloud services off the Cloud Service List; as such, the specific method of contracting varies depending on characteristics of each project. South Africa does not have a cloud marketplace or preapproved list. Each procuring agency has the flexibility to conduct procurements and contracting as they see fit, in accordance with the DPISA's *Determination and Directive*.

> > >

TABLE 2.4 - Summary of Procurement Models of the Case Studies

Case study	Model	Strengths	Weaknesses
Australia	Marketplace	<ul style="list-style-type: none"> • A marketplace offers a centralized location for procuring agencies to review cloud services with and without preapprovals or certifications. • There is flexibility in <i>how</i> to add CSPs and their cloud services onto a marketplace, <i>how</i> procuring agencies can select and contract with a CSP, and <i>how</i> to approach pricing and payments. 	<ul style="list-style-type: none"> • Requires advanced e-government capabilities to create and maintain an online marketplace.
UK			
Dubai			
Japan	Preapproved List	<ul style="list-style-type: none"> • Lists of preapproved CSPs offers procuring agencies an easy way to locate secure cloud services. 	<ul style="list-style-type: none"> • Procurements off the preapproved lists are conducted on a case-by-case basis, meaning there

Table 2.4 continued

Case study	Model	Strengths	Weaknesses
		<ul style="list-style-type: none"> Procuring agencies can engage in typical procurements such as tenders for cloud services on the preapproved lists. 	are no standardized contract templates available.
South Africa	Top-level Guidance	<ul style="list-style-type: none"> Procuring agencies must abide by the DPSA's <i>Determination and Directive</i>. This system provides flexibility in procurement methods for each agency. 	<ul style="list-style-type: none"> May result in discrepancies in security and service standards across the public sectors.

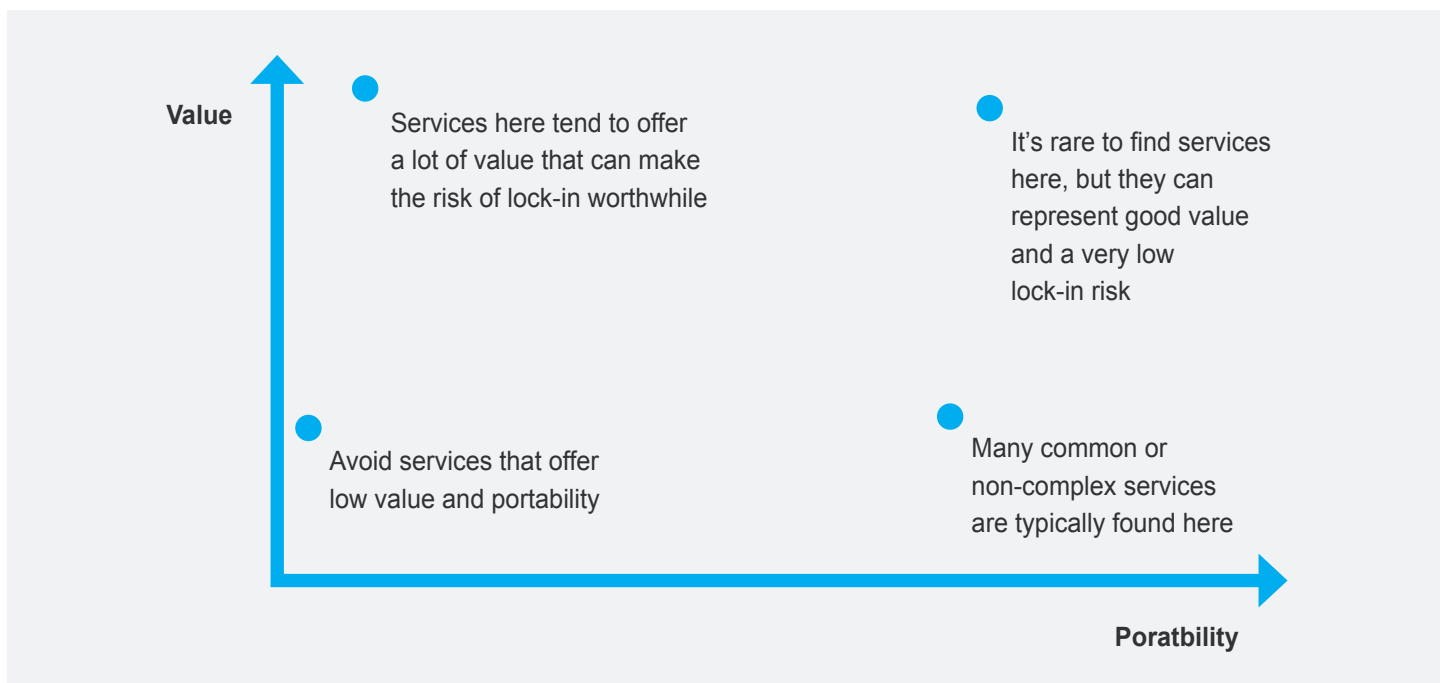
2.3.2 Managing Vendor Lock-in

Vendor lock-in is also a key consideration. Short-term cloud services contracts are one effective tool for managing the risk of lock-in. For example, the UK government's G-Cloud Framework contracts normally do not exceed 24 months. Similarly, most Australian procuring agencies buy subscription-based units of cloud services for no longer than three years.

The UK Central Digital and Data Office (CDDO) also calls on procuring agencies to assess which CSPs maximize both the value and portability of the services. Portability refers to the ease and affordability of moving a system and data from one CSP to another. More portable offerings decrease vendor lock-in risk. Agencies should consider portability ease and costs as part of its cloud service procurements. Figure 2.3 below illustrates how procuring agencies may assess CSPs based on their value and portability.

> > >

FIGURE 2.3 - Portability and Value Considerations for Cloud Services³²



Source: www.gov.uk.



2.3.3 Payment Methods

Some case studies also address pricing and payment considerations to enable transparent and fair cloud prices.

For example, the UK's Call-Off contract requires the procuring agency and vendor to specify the payment method, schedule of payments, and a breakdown of charges. Australia's DTA specifies that vendors cannot charge more than its maximum price posted on the Cloud Marketplace.

AWS's Cloud Procurement: Best Practices for Public Sector Customers offers numerous considerations for public sector payment methods for cloud services.³³

Some top considerations include:

- **Transparency:** CSP pricing information should be available and easy to understand for procuring agencies.

- **Variable Prices:** Cloud procurement models should allow flexibility to ensure cloud prices can fluctuate based upon market pricing, taking advantage of price reductions in the cloud market.
- **Multiple Pricing Models:** CSPs should be able to offer different pricing models to enable procuring agencies to assess which model best fits its needs.
- **Pay-Per-Use Model ("Utility Style"):** Countries should develop an on-demand, pay-as-you-go – utility style – option for procuring cloud services to help reduce costs.

See Appendix 2 for a one-page Comparative Analysis Table for the five case studies.



The Way Forward – Main Takeaways

Moving forward, readers are encouraged to use the findings of this report when deliberating on future plans for procurements of secure cloud services. Based upon the “lessons learned” above, key takeaways from this report include:

Institutional Coordination Mechanisms

Cloud First Principles and Top-Level Policy Guidance. Establishing a government-wide cloud first principle and outlining the government’s vision and objectives for using cloud services in government can help foster a standardized approach for preapproving CSPs and their cloud services. Government leaders are encouraged to leverage expertise across the bureaucracy, including cybersecurity and procurement specialist, to help develop these policies. See Box 3.1 below for suggested cloud first policy language.

> > >

BOX 3.1 - Suggested Language for a Cloud First Policy

“When procuring new or existing services, public sector organizations should consider and fully evaluate potential cloud solutions as the first option before exploring any alternative options such as on-premises infrastructure.

When choosing cloud models for procurement, agencies should consider and fully evaluate the public cloud as the first option before exploring any alternative cloud deployment models such community, hybrid, or private cloud.”

Source: World Bank.

Policies should be complemented by strong leadership and inter-governmental coordination. A motivated cadre of leaders within the government to provide guidance and enforce compliance is necessary to actually enact the policies. Moreover, the concept of change management to help foster the buy-in of government employees on public cloud solutions is also an important ingredient to success.

Institutional Framework. Considerations may include designating a central cybersecurity body to facilitate the preapproval of CSPs and their cloud services. This body would be responsible for overseeing cloud security

assessment activities and provide advisory and technical support to agencies, CSPs, and other stakeholders such as third-party assessors (3PAs). Countries may also consider establishing a cloud procurement office (CPO) to facilitate the procurement of cloud services, such as the establishment of a cloud marketplace or web-published list of preapproved CSPs to help facilitate procurements of cloud services. Some countries may have the capacity to establish these new offices, while others may be better aligned to designate existing offices to working groups to address CSP preapproval and procurement policies.

> > >

TABLE 3.1 - Example of a Responsibility Matrix for Institutional Framework of Cloud Preapproval and Procurement

Entity	Responsibility
A Top Policymaking Structure (such as a Cabinet Office)	Establish top-level policies and outline the vision and objectives for using cloud services in government.
A Central Cybersecurity Body	Develop and oversee data classification scheme and a preapproval process for CSPs and their cloud services.
Cloud Procurement Office	Establish a cloud procurement framework (such as a marketplace, preapproved list, hyperscaler agreement frameworks, etc.).

Source: World Bank.

Data Classification and Security Framework

Data Classification Framework. Most countries have already established a government-wide data classification scheme based upon CIA requirements. The data classification schemes typically include both government data and any personal data of its citizens (i.e., personally identifiable information, or PII³⁴) that it handles.³⁵ The *Data Classification Matrix and Cloud Assessment Framework* provides a suggested framework for how to align data classification schemes with key issues such as the type of systems to be procured – for example, on-premise computing versus public cloud, data residency requirements, and the rigor of preapproval activities. Ultimately, each procuring agency is responsible for using the government's data classification scheme to help understand its cloud security needs depending on the data and information environments.

Data Residency. A major consideration for every country is its data residency requirements for cloud services handling certain data classification levels (e.g., Official, Secret, or Top Secret). For example, a country may not have strict data residency requirements for CSPs handling data below its Official data classification level.³⁶ Moreover, procuring agencies handling Secret or Top Secret data typically require the use of private or community clouds. See the *Data Classification Matrix and Cloud Assessment Framework* for additional guidance.

The underlying reason for such residency requirements is the heightened concerns for cybersecurity and the notion that on-

premises or private cloud data will be more secure. Typically, these concerns relate to data on defense, geopolitics, diplomacy, strategic economic assets, and citizens. Governments could carefully evaluate these concerns according to their context, but the contrary may be true – public cloud might be safer. The rationale is simple. The data on-premises in a single centralized location can increase privacy and security vulnerabilities as it is more susceptible to a single point of failure. In contrast, a globally connected cloud creates economies of scale. Hyperscalers like Microsoft, Google, Amazon and others have teams of thousands of global cybersecurity experts working to safeguard the cloud by leveraging datapoints and data threats from all over the world. Microsoft experts, for example, monitor eight trillion security signals every 24 hours,³⁷ far more signals than any one customer would have access to with a local or private cloud. “The cybersecurity world offers lessons on why data localization and residency restrictions can be harmful and costly: Data security issues can arise from storing all data in one geographical territory, which is contrary to the diversification approach most commonly mandated in the cybersecurity industry and often adopted by multinational companies to ensure robust security across a geographically dispersed network.”³⁸

While there may be instances where the benefits of increased security are outweighed by another consideration, a government can only make that determination if it has a clear view on the potential benefits and risks. The example of Ukraine in Box 3.2 below is an excellent example.

> > >

BOX 3.2 - How Cybersecurity Concerns in Ukraine Led to the Migration of Government Data to Public Cloud

Prior to the war with Russia, Ukraine had a long-standing Data Protection Law that prohibited government authorities from processing and storing data in the public cloud. This meant that the country's public-sector digital infrastructure was run locally on servers physically located within the country's borders. A week before the war started in 2022, the Ukrainian government was running entirely on servers located within government buildings—locations that were vulnerable to attacks.

Ukraine's Minister of Digital Transformation and his colleagues in Parliament recognized the need to address this vulnerability. On February 17, 2022, days before the start of the war, Ukraine's Parliament amended its Data Protection Law to allow government data to move off existing on-premises servers and into the public cloud. This in effect enabled it to “evacuate” critical government data outside the country and into data centers across Europe. Microsoft and other tech companies rallied to help. Within 10 weeks, Ukraine's Ministry of Digital Transformation and more than 90 chief digital transformation officers across the Ukrainian government worked to transfer to the cloud many of the central government's most important digital operations and data.

The data was the target of intensely heightened cybersecurity attacks during the war. However, recent advances in cyber threat intelligence and end-point protection have helped Ukraine withstand a high percentage of destructive cyberattacks. Cybersecurity experts noted multiple waves of destructive cyberattacks against 48 distinct Ukrainian agencies and enterprises, seeking to penetrate network domains by initially compromising hundreds of computers and then spreading malware designed to destroy the software and data on thousands of others.

A defining aspect of Ukraine's defense so far has been the strength and relative success of its cyber defenses supported by private sector companies like Microsoft. While not perfect, and some destructive attacks have been successful, these cyber defenses have proved stronger than offensive cyber capabilities. This reflects two important and recent trends. First, threat intelligence advances, including the use of artificial intelligence, have helped to make it possible to detect these attacks more effectively. And second, internet-connected end-point protection has made it possible to distribute protective software code quickly to cloud services and other connected computing devices to identify and disable malware. Ongoing wartime innovations and measures with the Ukrainian Government have strengthened this protection further. But continued vigilance and innovation will likely be needed to sustain this defensive advantage.

Source: "Extending our vital technology support for Ukraine," Microsoft On the Issues, November 3, 2022; "Defending Ukraine: Early Lessons from the Cyber War," Microsoft On the Issues, June 22, 2022; Microsoft Digital Defense Report 2022 (released June 22, 2022); "An overview of Russia's cyberattack activity in Ukraine," April 27, 2022.

In March 2022, following cyberattacks on Ukraine, the Government of the Republic of Lithuania approved amendments to the Law on Management of State Information Resources³⁹ with the aim of improving security and resiliency of government services by allowing storage of additional copies of government data to be held in data centers located in the European Union (EU), the North Atlantic Treaty Organization (NATO), or the European Economic Area. Such data centers will have to meet the same technical requirements for cyber security and national security interests as national data centers. The law had previously required that state data only be stored in national data centers.

Some smaller countries may have difficulty attracting CSPs to build data centers within their geographical boundaries. One possibility to address this challenge is a "trusted neighbor" concept whereby countries can host government data within CSP data centers located within trusted neighboring countries or allies. Moreover, with regard to data sovereignty, CSPs are bound by national legal requirements of their countries. For example, American CSPs and any CSP with a US subsidiary is currently bound by the requirements of the *CLOUD Act*.⁴⁰ Within this context, countries' decisions on adopting public cloud services should be informed by conversations with CSPs to understand their legal obligations for their national governments, especially for sensitive data of citizens such as PII.

Security Controls based upon International Standards.

There are various approaches to establishing security controls for the preapproval of CSPs.

- A country can consider leveraging international standards, such as ISO/IEC and CSA security controls, as the basis for preapproving CSPs. Both ISO/IEC and CSA certifications are highly respected, widely used global cybersecurity standards that many CSPs already possess. It is much simpler and easier for countries to verify a CSP's existing certification with these international standards instead of creating a new set of security controls. This is the preferred method for developing countries.
- Alternatively, developed countries may consider a more advanced, *tiered* security framework to preapprove or certify CSPs based upon the classification level of the data to be handled. One example of this method is the US government's FedRAMP system.
- Regardless of the security control path chosen by the country, a cybersecurity body or a group of government cybersecurity experts can lead the development of the preapproval framework using the *Data Classification Matrix and Cloud Assessment Framework* as guidance.

Security Assessments. Countries are encouraged to facilitate a standardized approach to preapprove CSPs to handle certain government data, whether by a government agency, an accredited third-party assessor (3PA), the cybersecurity agency, or a combination thereof. As noted above, this could be done using international security control standards (a more simplified approach) or a tiered security framework (a more advanced approach).

- If multiple countries adopt the same international standards such as ISO/IEC and CSA certifications, this could enable the harmonization of security assessments across countries.
- Countries should also consider the concept of “inheritance,” whereby every layer of the cloud stack is certified. This means if a SaaS is built upon a certified PaaS or IaaS, an assessor only assesses the SaaS. This eases the certification process of SaaS providers.

Local CSPs vs Hyperscalers. Hyperscalers have generally already implemented international security standards such as ISO/IEC and CSA, which gives them an edge over local CSPs identified as small and medium-sized enterprises (SMEs) in terms of government contracts. A standardized security framework and associated requirements such as inheritance of controls could help address this challenge and provide local SMEs to register as eligible providers.

Continuous Monitoring. Procuring agencies are ultimately accountable for the security of their IT enterprises. As such, they are responsible for working with CSPs to maintain a secure public cloud environment. In this regard, agencies, CSPs, and others (such as 3PAs) are encouraged to work together to continuously monitor the security of the cloud environment and operation. Government and commercial stakeholders should be responsible for notifying each other of any security incidents, and such incident reports should be elevated to a country’s central cybersecurity body. Agencies may also seek to request CSPs to connect with their incident monitoring platforms to guarantee the security of their cloud solutions. Other suggestions include annual or biennial recertifications and security control change notifications by the CSPs.

Procurement Arrangements

Centralized Marketplace or Listing for Cloud Services. An online marketplace of CSPs and their cloud solutions for

procuring agencies may be considered. Under this system, a CSP would be expected to sign a general Cloud Framework Agreement as a condition of joining the marketplace that includes basic cybersecurity and data privacy provisions (such as compliance with relevant national laws) that can be verified by the country. The Cloud Framework Agreement would require periodic updates, based upon the limits of the relevant procurement legislation for framework agreements in the countries and other considerations. Marketplaces typically include pricing for each cloud service offering and clearly identify a CSP’s preapproval or certification status.

Alternatively, countries may instead establish a listing of preapproved CSPs and their cloud services that is easily accessible to procuring agencies. Countries may also consider setting up Master Agreements with hyperscalers that offer special terms and pricing for hyperscaler offerings available to all procuring agencies for direct contract awards or tenders. Such agreements should also include basic cybersecurity and data privacy provisions. Under this setup, a procuring agency could directly purchase basic cloud services from hyperscalers, as opposed to buying these services at higher cost through resellers on the marketplace.

Selecting a Cloud Offering. The above recommendations allow procuring agencies to review cloud offerings on the marketplace or preapproved list/registry to determine which CSPs meets their specific business and security requirements. The *Data Classification Matrix and Cloud Assessment Framework* provides a possible template for agencies to assess their own internal business and security needs.

Procuring agencies can leverage numerous ways to begin a procurement of a selected cloud service. For example, a procuring agency may issue a tender or RFQ to facilitate competitive bidding between CSPs on the marketplace. A procuring agency may also consider choosing a cloud service based on a best value standard that considers cost, security, total cost of ownership, and other relevant considerations. Other procurement considerations may include the capacity of a cloud solution to scale services, the ease of receiving desktop support from CSPs, and the costs of capital expenditures (CapEx) versus operating expenditures (OpEx). Another consideration is whether or not the procurement involves data migration from legacy systems or applications, as presented below in Box 3.3. Ultimately, the cloud service selections are determined by the needs of each procuring agency.

> > >

BOX 3.3 - Data Migration Considerations – Lessons from Singapore

There are numerous considerations to be made on data migration related to the cloud, whether it be migrating data from a legacy system into a cloud environment or from an existing cloud vendor to another cloud vendor. Some good practices in this area include:

- When transitioning from a legacy system or application, it is helpful to plan for a separate cloud expert support services contract for a system integrator to support procuring agency with their acquisition planning.
- When transition between cloud vendors, it is important to establish data migration requirements within the contract agreements (see Box 3.4).
- In either case, procuring agencies should take the opportunity to inventory data and erase or archive unneeded data before a transition. Furthermore, procuring agencies should work with vendors to ensure a secured and seamless data migration process.

Singapore provides a helpful example by outlining different approaches to data migration. The Singapore government uses four approaches for data migration, each of which has cost-benefit trade-offs:

1. **Rehost:** A lift-and-drop approach, migrating workloads from on-premises to cloud with minimal changes to the application. This approach can be used for legacy systems that would be redeveloped in the short run as well as simple and agency-specific systems that do not require frequent changes. (Low level of realized benefits)
2. **Re-platform:** Migrate workloads to run on cloud with some changes to modernize critical components like middleware and/or database. This approach can be used for legacy systems that are required to operate in the medium-term before full redevelopment, simple, agency-specific systems that do not require frequent changes, and systems in the middle of their life-cycle. (Medium level of realized benefits)
3. **Redevelop:** Redevelop apps to take advantage of cloud-based technologies, such as containers and serverless runtime. This approach can be used for systems that need to fully exploit the capabilities on the Cloud and have more unique needs. (High level of realized benefits)
4. **Replace:** Replace with SaaS, which are licensed on a subscription basis and hosted on the cloud. This approach can be used for enterprise systems with a high degree of functional commonality and low degree of customization. (Medium-high level of realized benefits)

Singapore has a team of developers who have created “Open API” (Open Application Programming Interface) solutions to help move data between systems. Singapore works to ensure CSPs can interoperate with the Open APIs. Overall, this approach allows Singapore to move data more easily between systems, which improves data migration efforts.

Source: Richard Tay, Senior Director, Government Infrastructure Group, Government Technology Agency, Singapore.

Simplified and Standardized Contracts. Simple and standardized contracts are the preferred method for procuring cloud services. Box 3.4 below offers considerations for

developing a standardized Call-Off Contract template for contracting with CSPs on a marketplace.

> > >

BOX 3.4 - Considerations for a Call-Off Contract Template for a Cloud Marketplace

The Contract Template should provide (1) the basic details such as parties and contract period, (2) terms and conditions of the cloud service, and (3) data security and privacy conditions. The list of considerations to be included in this template could therefore include:

- An Order Form that includes contracting parties, start and end date, extension possibilities, contract value, pricing model, payment method, and invoice details.
- A Service Level Agreement (SLA) that details performance details listing the seller's obligations, including quality of services requirements, along with provisions for rebates if there is a failure of service.
- Statement of the division of responsibilities between the buyer and seller for the information system, including data custodianship responsibilities.
- Requirement for the seller to abide by relevant national laws, agency regulations, and applicable international standards.
- Statement of data ownership rights of the buyer.
- Description of usage rights and intellectual property rights, including requirements that seller provides the buyer with certain usage and intellectual property rights of the cloud service during the contract period.
- Statement of the seller's insurance along with the seller's liability requirements to the buyer.
- Dispute resolution provisions.
- The seller's exit plan to ensure orderly transition to a new seller, including the rights of the buyer for early termination and a requirement to erase or archive specified data as part of the contract termination.
- Listing of current cybersecurity certifications and/or cybersecurity standards followed; operative data privacy standards; and location of data storage, processing, and transit.
- Requirement for the seller to notify the buyer of a security breach.
- Requirements for continuous security monitoring.

An example of a cloud marketplace contract template provided by the UK Crown Commercial Office's G-Cloud Framework and Call-Off Contract Templates (see Footnotes 103, 107).

Sometimes, more complex solutions with specific functional requirements not available on the marketplace could necessitate tenders or RFQs outside the marketplace. In

these cases, a procuring agency would conduct functional evaluations of specialized cloud services off the marketplace.

Regardless of the type of contract, each contractual agreement with a CSP should clearly state that the procuring agency is the data owner, while the CSP is the data custodian. The procuring agency should also detail how the CSP should archive its data during or after the contract period as well as how to handle the government-owned data at the conclusions of the agreements—for example, erasing or migrating the data.

Avoiding Vendor Lock-in. Short-term contracts, usually two-year contracts or less with limited annual renewals, help to manage the risk of vendor lock-in. Procuring agencies should also be aware of portability fees – the cost of transferring data from one CSP to another – before signing a contract. The lower the portability costs, the lower risk of vendor lock-in. Procuring agencies should also consider listing cloud portability tools and associated migration as optional services in the tenders or RFQs. Such services would help the procuring agencies to migrate between CSPs more easily.

Payment Methods. Procuring agencies should choose a payment method that best fits their situation, depending on the specific project needs. Key considerations for obtaining fair cloud prices include promoting pricing transparency, allowing cloud service prices to fluctuate based upon market prices, allowing CSPs to offer different pricing models, and creating an on-demand, pay-as-you-go (utility style) payment option. Indeed, many procurers prefer to begin using the pay-as-you-go model for initial procurement of cloud services

as opposed to more expensive fixed-price contracts. In this way, the procuring agencies would purchase a cloud offering as a service contract—not a product purchase. In addition, Master Agreements with CSPs (especially hyperscalers) for cloud services across multiple government agencies can help reduce costs for countries.

Furthermore, donor-funded projects face issues of disbursements – monthly subscriptions will slow down disbursement – and potential inability of the government to pay for the cloud subscription fees once the project is closed. Advance payment for up to three years of subscription fee is allowed by vendors like AWS. This could be considered to address the issues of slow disbursements and government's potential default on subscription payments after the project's closure.

Appendix 1 provides a Step-by-Step Guide for countries to consider when beginning the journey to public cloud procurements.

Governments and their procuring agencies may wish to adopt the above recommendations to manage the risks of procuring public cloud services. These cloud solutions can be interoperated with other cloud deployment models—such as GovClouds—to facilitate a trusted Hybrid Cloud environment for governments. See Box 3.3 for more information on different interoperating cloud environments through Open API.



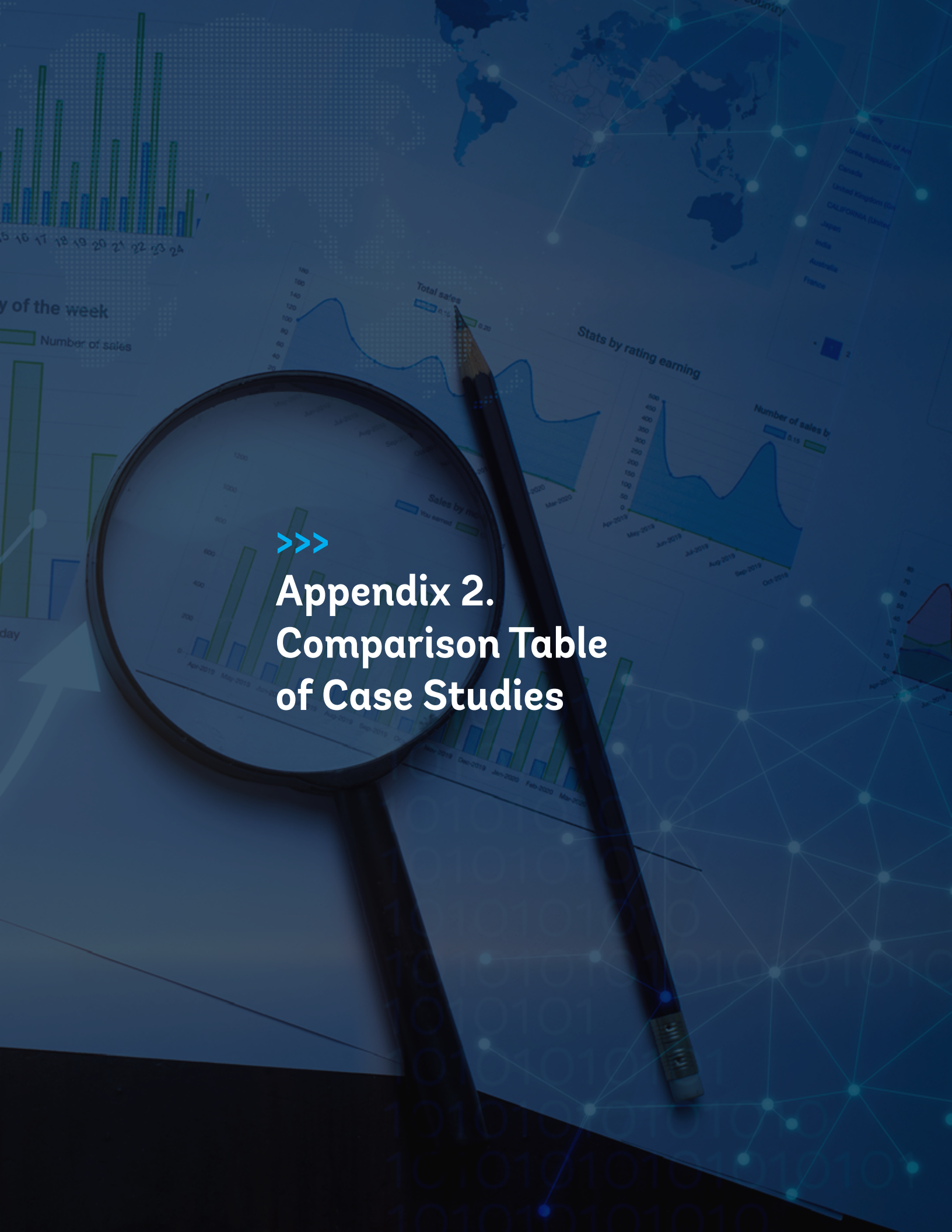
Appendix 1. Step-By-Step Guide to Public Cloud Assessments and Procurements for Government







Appendix 2. Comparison Table of Case Studies



Metrics	Japan	Australia	UK	South Africa	Dubai
Institutional Coordination Mechanisms					
Cloud First Principle?	Yes	Yes	Yes	Yes –through a regulatory order, not a national policy	Yes
Institutional Framework	Centralized Model	Hybrid Model	Hybrid Model	Decentralized Model	Hybrid Model
Data Classification and Security Framework					
Data Classification	ISMAP considers one data classification level: Confidential 2	Unclassified (Unofficial, Official, Official: Sensitive) Classified (Protected, Secret, Top Secret	Official Secret Top Secret	Restricted Confidential Secret Top Secret	OPEN SHARED-Confidential SHARED-Sensitive SHARED-Secret
Data Residency	Risk-based decision recommended for each agency	Risk-based decision recommended for each agency handling sensitive and classified data	Risk-based decision recommended for each agency	Public cloud data must always reside within the borders of South Africa (with limited exceptions)	Handling of SHARED data outside the UAE is prohibited
Security Controls	Japanese Industrial Standard (JIS) (based on ISO 27000 family)	Cloud Security Controls Matrix (based on NIST SP 800-37)	None required; <i>14 Cloud Security Principles</i> recommended	Refers to national laws and agency-specific information security requirements	CSP Security Standard (based on ISO 27000 family and CSA Cloud Controls Matrix)
Security Assessments	Uses third-party “ISMAP Assessors” for CSP security assessments	Uses third-party “IRAP Assessors” for CSP security assessments	UK’s G-Cloud Framework requires CSPs to self-declare cybersecurity and data privacy-related information	Each procuring agency assesses CSPs based upon national and departmental information security standards	Uses third-party “Certification Bodies” for CSP security assessments
Continuous Monitoring	Annual reassessments for CSPs on the ISMAP Cloud Service List	Reassessments every 24 months for IRAP-approved CSPs and their cloud services	24-month maximum G-Cloud Contract	Contracts cannot exceed 5 years	Basic reviews every 12 months and full re-certifications every three years

Metrics	Japan	Australia	UK	South Africa	Dubai
Procurement Arrangements					
Procurement Model	"Cloud Service List"	"Cloud Marketplace"	"Digital Marketplace"	Agency-specific	"eSupply"
Selecting CSPs	Open Tendering system on the ISMAP Cloud Service List	Competitive bidding process (RFQ) within Cloud Marketplace	Selection off the Digital Marketplace	Follows the requirements of <i>Public Service Cloud Computing Determination and Directive</i>	Selection off the eSupply
Contracting Methods	Case-by-case	Contracts under the Cloud Marketplace panel arrangement	Call-Off Contracts under G-Cloud Framework	Follows the requirements of <i>Public Service Cloud Computing Determination and Directive</i>	Case-by-case



Annex 1. **Japan's ISMAP Program**

1. Brief History and Background of Japan's Cloud Security Governance

Over the past five years, the Japanese government has established new policies to promote government adoption of commercial cloud services. Most notably, the Japanese government adopted the *Cloud Adoption Policy for Government Information Systems* in June 2018. This policy promoted a cloud-by-default or cloud first principle that calls on procuring agencies to prioritize cloud adoption over on-premises computing networks.⁴¹

The Japanese government has also developed new cybersecurity policies. For example, Japan's June 2018 *Future Investment Strategy* and the July 2018 *Cybersecurity Strategy* both promote cybersecurity evaluations of cloud services for public use.⁴²

In response to the need for secure cloud services, Japan's **Ministry of Internal Affairs and Communications (MIC)** and **Ministry of Economy, Trade and Industry (METI)** organized the "Study Group on Security Assessment of Cloud Services" from August 2018 through December 2019.⁴³ In January 2020, the Study Group issued a report on its findings, which called for a centralized system to preapprove cloud services.

Also in January 2020, Japan's **Cybersecurity Strategy Headquarters** established the *Basic Framework of the Security Assessment System for Cloud Services in Government Information Systems*, which developed a

centralized approach toward cloud security governance for procuring agencies in Japan, called the Information System Security Management and Assessment Program (ISMAP).⁴⁴ Under the *Basic Framework*, the ISMAP system administers the government's preapproval process for cloud procurements, similar to the FedRAMP program in the United States.

In June 2020, the Japanese government began ISMAP operations and published the *Basic Regulation for ISMAP*, which outlines the framework for cloud service preapproval activities.⁴⁵

2. Institutional Coordination Mechanisms

ISMAP is a centralized government-led system that aims to streamline the Japanese government's preapproval process for commercial cloud services for procuring agencies. Japan's Basic Regulation for ISMAP and supporting documents detail the roles for all organizations involved in ISMAP.

Key Organizations

The **Cybersecurity Strategic Headquarters** ("the Headquarters") was established by the 2014 *Basic Act on Cybersecurity*. The Headquarters is responsible for promoting Japan's cybersecurity and is chaired by the Chief Cabinet Secretary.⁴⁶ It also decides the *Basic Framework* for the ISMAP system.



Under the *Basic Framework*, the **National Center of Incident Readiness and Strategy for Cybersecurity (NISC)**, the **Digital Agency**, **MIC**, and **METI** are responsible for administration and operation of ISMAP.

- **NISC** collaborates with industry, academia, as well as the public and private sectors to promote cybersecurity in Japan, including the oversight of ISMAP.
- The **Digital Agency** (previously the National Strategy Office of Information and Communications Technology), **MIC**, and **METI** are government ministries that also support the administration and operation of ISMAP.

The *Basic Framework* also defines two organizations responsible for decision-making and operation of ISMAP:

- **ISMAP Steering Committee** is the highest organ of decision-making for the operation of ISMAP. It establishes the rules for ISMAP and is in charge of the general operations of ISMAP. The Headquarters has designated NISC as the secretariat of the ISMAP Steering Committee.
- **ISMAP Operations Support Organization** handles the administrative tasks of the ISMAP Steering Committee. The Japanese government has designated the **Information-technology Promotion Agency (IPA)** as the ISMAP Operations Support Organization. In this role, IPA provides practical and technical support for ISMAP operations.
- IPA assigns responsibility for the evaluation and management of ISMAP Assessors to the **Japan Information Security Audit Association (JASA)**.

ISMAP Assessors are third-party organizations (typically companies) responsible for conducting information security assessments on cloud services under application for ISMAP certification. A company must request the ISMAP Steering Committee to be registered on the “Approved Assessor List.”⁴⁷ After being assessed by JASA and added to this list, the ISMAP Assessor may conduct security assessments on behalf of ISMAP. As of July 2022, there are five ISMAP Assessors on the Approved Assessor List.⁴⁸

Japanese government agencies (or “procuring agencies”) procure cloud services offered within ISMAP. Procuring agencies are responsible for issuing tenders for cloud services on the “ISMAP Cloud Service List.”⁴⁹ As of July 2022, there are 38 cloud services – also called cloud service offerings (CSOs) – from 27 CSPs on the ISMAP Cloud Service List.

Coordination Among Organizations

Japan’s *Basic Regulation for ISMAP*⁵⁰ and its supporting documentation have created the framework governing the coordination among the various organizations involved in ISMAP.

Overall, the Japanese government promotes a centralized system wherein ISMAP is responsible for cybersecurity assessments of cloud services. Approved cloud services are added to the ISMAP Cloud Service List, from which procuring agencies can issue Tenders.

The Headquarters sets the *Basic Framework* policy creating ISMAP. In turn, NISC, the Digital Agency, MIC, and METI report on the system operation status to the ISMAP Steering Committee, which decides on items such as registrations to the ISMAP Assessor List and the ISMAP Cloud Service List.

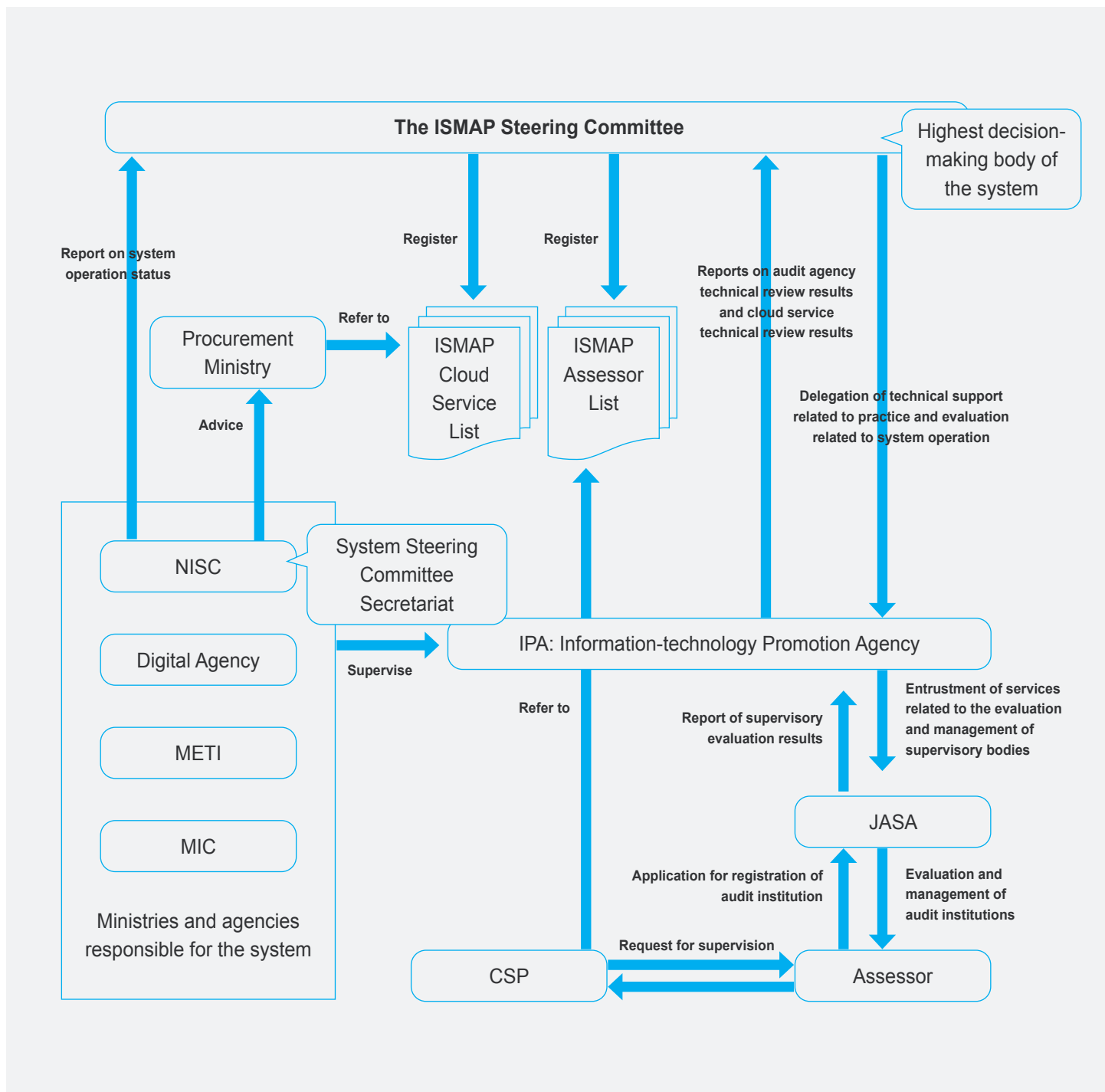
The ISMAP Steering Committee is the ultimate decision-maker on additions to the ISMAP Assessor List and ISMAP Cloud Service List. The ISMAP Steering Committee delegates technical and operational activities to IPA, which reports to the ISMAP Steering Committee on the results of the technical evaluations of Assessors and CSPs. IPA delegates its reviews of ISMAP Assessors to JASA.

To register ISMAP Assessors, JASA provides an evaluation report of a potential assessor to IPA, which in turn submits its report to the ISMAP Steering Committee. The evaluation report helps the ISMAP Steering Committee to decide whether or not to register a company onto the ISMAP Assessor List.

To assess cloud services, CSPs must select an assessor from the ISMAP Assessor List to conduct a security assessment of its proposed cloud service. The ISMAP Assessor provides its assessment report to the CSP and then the CSP submits the report to the IPA with relevant application documents. The IPA conducts technical evaluation of the cloud service based on the assessment report and application documents, and submits an examination report to ISMAP Steering Committee with its opinion on whether or not to register the cloud service.

The ISMAP Steering Committee has the ultimate discretion on whether or not to register the cloud service onto the ISMAP Cloud Service List, based upon the IPA’s technical evaluation report of the cloud service (Figure A1.1). In turn, procuring agencies may issue a tender for cloud services on the ISMAP Cloud Service List.

FIGURE A1.1 - Basic Framework of ISMAP



Source: [ISMAP](#).

3. Data Classification and Security Framework

The Japanese government has developed a security framework to support ISMAP's preapproval process and procurement of secure cloud services. The Japanese government's data classification framework supports the ISMAP's preapproval process. The ISMAP process also provides a robust process to preapprove the cybersecurity of a cloud service by adding it to the ISMAP Cloud Service List.

Data Classification

The Japanese government uses only one data classification type for ISMAP: "Confidential 2" information. This data classification level is the most frequently used by the Japanese government. Confidential 2 corresponds to the "Moderate" Impact Level of the US government's FedRAMP, which is defined by the **National Institute of Standards and Technology (NIST) FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems** as:

"The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals....A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (1) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (2) result in significant damage to organizational assets; (3) result in significant financial loss; or (4) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries."⁵¹

Data Residency

Japan's data residency posture is based upon two key policies:

- "Basic Policy on Usage of Cloud Service for Governmental Information Systems" (September 10, 2021) calls on the use of cloud services that operate data centers in locations where Japanese laws and treaties have jurisdiction.
- "Common Standards for Cybersecurity Measures for Governmental Agencies" (July 7, 2021) notes that agencies should assess risks resulting from the handling of data in places under foreign jurisdiction.

Overall, these two policies require procuring agencies to strongly consider the potential risks of the handling of data that may become subject to foreign laws and regulations when selecting cloud service offerings.

Security Controls

ISMAP developed its security controls under the assumption that cloud services will handle data classified as "Confidential 2" information. The security controls are based upon *Japanese Industrial Standard (JIS) Q 27001, 27002, 27014, 27017*, which correspond to the ISO/IEC family, *Japan's Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies*, and FedRAMP Moderate controls based upon NIST 800-53 (Rev. 4).⁵²

The ISMAP Steering Committee published the Control Criteria of ISMAP in June 2020 (updated in April 2022),⁵³ which organizes ISMAP controls around three criteria:

- **Governance Criteria.** ISMAP's Governance Criteria guide review of a CSP's ability to guide and manage its information security activities of its organization. These criteria are based upon JIS Q 27014:2015 controls, which are closely aligned with ISO/IEC 27014:2013.
- **Management Criteria.** ISMAP's Management Criteria guide the of review a CSP's ability to establish, implement, operate, monitor, maintain, and improve its information security management. These criteria are based upon JIS Q 27001:2014 controls, which are closely aligned with ISO/IEC 27001:2013.
- **Operation (or 'Controls') Criteria.** ISMAP's Operation Criteria determine a CSP's technical security requirements (e.g., access controls) typically implemented by its IT/cybersecurity team. These criteria are based upon JIS Q 27002:2014 controls, which are closely aligned with ISO/IEC 27002:2013, and JIS Q 27017:2016, which are closely aligned with ISO/IEC 27017:2015. ISMAP also maps its Control Criteria to NIST 800-53 (Rev. 4) and to *Japan's Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies*.

As illustrated in Figure A1.2, the three categories represent the flow of responsibility from the CSP's governing body (Governance Criteria) to its management team/administrators

(Management Criteria) (administrators) to its IT/cybersecurity professionals (Controls Criteria). Moreover, the number of controls increases for each category down the Criteria list.

> > >
FIGURE A1.2 - Structure of ISMAP’s Control Criteria



Source: [ISMAP](#).

Preapproval Process

The Japanese governments’ Basic Regulation on ISMAP outlines the preapproval process and requirements under ISMAP.⁵⁴ ISMAP has a four-step process for Japanese procuring agencies:

STEP 1, Development of Criteria. As noted above, ISMAP has developed Control Criteria for Confidential 2 information handled by Japanese procuring agencies. This framework uses three types of criteria covering Governance, Management, and Operation, respectively. ISMAP is responsible for regularly

updating these Control Criteria to ensure its security controls are up-to-date.

STEP 2, Pre-Procurement Examination. CSPs request ISMAP Assessors to conduct a security assessment of their cloud service based upon ISMAP’s Control Criteria. The Assessment Report is then submitted through the CSPs themselves to IPA and the ISMAP Steering Committee to review the entire cloud service application, including the Assessment Report, to determine whether or not to register the cloud service. If approved, the cloud service is registered onto ISMAP’s Cloud Service List.

STEP 3, Procurement. A Japanese procuring agency interested in procuring a cloud service first issues a tender for cloud services on the ISMAP Cloud Service List. CSPs can then respond to a Tender issued by a procuring agency. In turn, the Japanese procuring agency can enter into a procurement agreement with a CSP for its preferred cloud service on the ISMAP Cloud Service List.

STEP 4, Examination for Renewal. The effective registration period for a cloud service on ISMAP's Cloud Service List is 12 months.

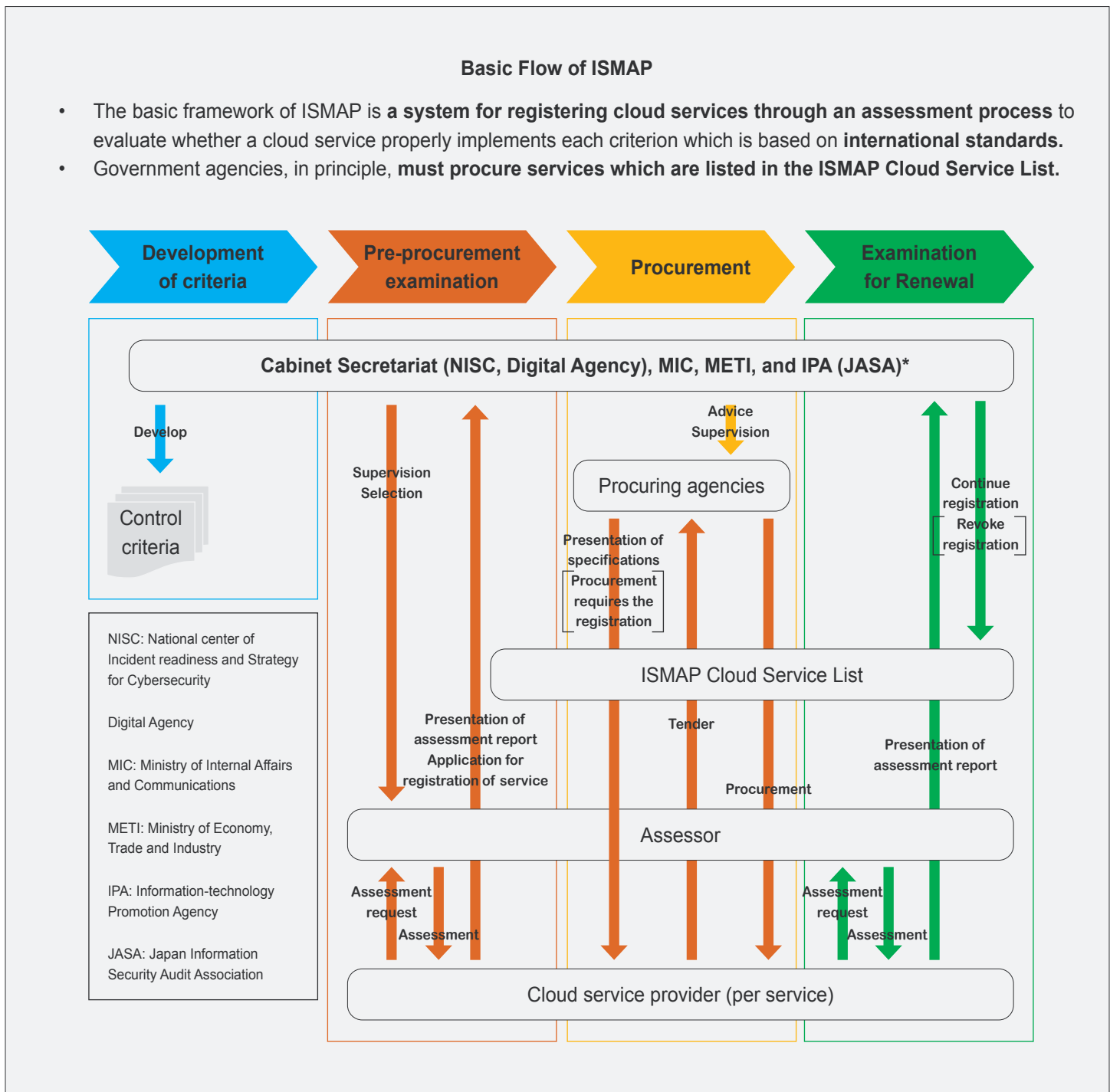
- CSPs must apply for the renewal of their cloud service registration by the end of the 12-month effective period, after receiving the assessment report from the ISMAP Assessor.
- The registration remains effective after the expiration of the 12-month effective period until such time that the ISMAP Steering Committee decides whether to continue or cancel the registration. This period lasts 16-months. It includes a 12-month assessment period of the CSP, a three-month preparation period for the assessment report of ISMAP Assessor, and a one-month preparation period for the CSP's application.

- The renewal process is meant to provide regular reviews of each cloud service's security posture and fidelity to ISMAP's Control Criteria.

Each CSP must also report to the ISMAP Steering Committee without delay when there are changes to the information of its cloud service described in the ISMAP Cloud Service List, or when there are significant control changes or circumstances that could result in such changes to its cloud service during the 16-month period.

In addition, CSPs must immediately send a summary report to the ISMAP Steering Committee if there is an information security incident which could have a significant impact on cloud service users. In such a case, the ISMAP Steering Committee may request the CSP to have an Assessor conduct a reassessment of the CSP's cloud service. Based upon the results of the Assessment, the ISMAP Steering Committee may continue or cancel the cloud service's registration on the ISMAP Cloud Service List. Similarly, the effective registration period for an Assessor on ISMAP's Assessor List is 24 months. Assessors must apply for the renewal of the registration by the end of the effective period.



FIGURE A1.3 - Four-Step Process of ISMAP

Source: [ISMAP](#).

Note: The IPA provides practical and technical support for operation, and cosigns evaluation, and management of assessor to JASA.

4. Procurement Arrangements

ISMAP outlines a process for procuring agencies to issue tenders for cloud services on the ISMAP Cloud Service List.

As noted above, **a Japanese procuring agency interested in purchasing a cloud service must issue a tender for cloud services on the ISMAP Cloud Service List to begin the procurement process.** Agencies generally employ an open tendering system: the agencies develop requirements, issues a Request for Tenders, conducts bidding and bid openings, examines the proposals from providers, and then enters into a contract with the chosen provider.

- Registration on the ISAMP Cloud Service List is generally considered a requirement for providers wishing to submit proposals.

- Cost evaluations depend on the type of contract. For example, procuring agencies seeking multi-year contracts evaluate the total cost of cloud services over the multiyear period. In addition, procuring agencies evaluate the unit price when purchasing cloud services on a “per account” basis (not a fixed quantity).

The specific method of contracting varies depending on characteristics of each project. Payment methods are also determined on a case-by-case basis by each procuring agency. Some additional considerations that procuring agencies may consider of the vendors during the procurement processes include female participation and advancement in the company’s workplace, support for childcare, and wage increase policies.

The background of the slide features a dark blue, semi-transparent image. It depicts a hand with a blue wristband pointing its index finger towards a globe. The globe shows a map of the world with a grid of latitude and longitude lines. A large, light blue star is positioned in the lower right quadrant of the image.

>>>

Annex 2. Australia's Anatomy of a Cloud Assessment and Authorization Framework

1. Brief History and Background of Australia's Cloud Security Governance

The Australian government's original cloud policy, the 2014 *Australian Government Cloud Computing Policy*, created a cloud first principle for procuring agencies and sought to reduce duplication and fragmentation of cloud services implementation.⁵⁵ This policy led to the creation of Australia's Cloud Services Certification Program (CSCP), administered by the Australian Cyber Security Centre (ACSC) under the Australian Signals Directorate (ASD). Under this system, ASD managed a "Certified Cloud Services List" (CCSL), from which government entities could select cloud services.⁵⁶

Starting in 2017, the Australian government began to reform its cloud security framework. In 2017, the Digital Transformation Agency (DTA) began coordinating with other government bodies to review the current system and develop a new *Secure Cloud Strategy* to replace the 2014 *Cloud Computing Policy*. Complementing this work, an ASD-led independent review found that the ASD did not have the capacity to certify every cloud service onto the CCSL in a timely manner. This centralized system created bottlenecks and undermined Australian procuring agencies' ability to fully leverage all cloud services being offered on the market.⁵⁷ In 2020, the ASD ceased CSCP activities and withdrew the CCSL as the government transitioned to the *Secure Cloud Strategy*.

In 2018, the DTA published the *Secure Cloud Strategy*,⁵⁸ last updated in September 2021, which is now the key policy document underpinning the Australian government's cloud consumption and aligns with ASD's cloud assessment and authorization system. The updated

strategy retains Australia's cloud first principle. Australia has also developed additional guidance to complement DTA's *Secure Cloud Strategy*, including:

- *Anatomy of a Cloud Assessment and Authorization*, which guides CSPs, cloud consumers, and IRAP assessors on the government's new cloud service assessment process.⁵⁹
- *Cloud Security Assessment Report Template*, which assists IRAP assessors in compiling the report required to evaluate and authorize a CSP.⁶⁰
- *Information Security Manual (ISM)*, which provides a cybersecurity framework that organizations use to protect their information and systems.⁶¹
- *Cloud Security Controls Matrix (CSCM)*, which complements the Cloud Security Assessment Report Template by providing information on cloud computing security controls.⁶²
- *Protective Security Policy Framework (PSPF)*, which provides mandatory guidance and obligations to ensure cloud services are suitable for the handling of government data.⁶³
- In addition to these publications, the ACSC features a series of Cloud Computing Security Considerations for CSPs and tenants.⁶⁴



2. Institutional Coordination Mechanisms

The Australian government has established a bureaucratic regime to support cloud security governance. The Australian government's *Anatomy of a Cloud Assessment and Authorisation* guidance document describes the institution coordination mechanism for its cloud security governance. The document outlines the key organizations responsible for cloud security, their relationships, and their key rules, regulations, and guidelines.

Key Organizations

DTA leads Australian government strategy and policy efforts related to information and communications technology (ICT) investments and digital service delivery.⁶⁵ DTA is responsible for the publication and periodic updates of the *Secure Cloud Strategy*, which promotes a whole-of-government strategy on secure cloud procurements that align with ACSC guidance. DTA also hosts the Australian government's **Cloud Marketplace** within its **BuyICT** Online Platform.

ASD leads Australia's intelligence, cybersecurity, and offensive cyber operations.⁶⁶ Within the ASD, **ACSC** works with industry, residents, and government organizations on matters related to cybersecurity incidents and threat mitigations.⁶⁷ ACSC provides guidance for cloud security, supply chain security, and gateway and cross domain guidance, among other things. Key ACSC publications related to cloud security include the *Anatomy of a Cloud Assessment and Authorization*, *Cloud Security Assessment Report Template*, *Cloud Security Controls Matrix*, *Cloud Computing Security Considerations*, and *Cloud Computing Security for Tenants*.

The **Attorney-General's Department** publishes guidance for government agencies. The Department's PSPF sets a number of government protective security policies that are integrated into the ACSC's *Anatomy of a Cloud Assessment and Authorisation* procedures.

IRAP Assessors are ICT professionals from either the private sector or the Australian government endorsed by ASD to provide information security services. To be certified as an IRAP Assessor, an ICT professional must undergo a certification review process conducted by the ASD, in which they must prove the following qualifications:

- Demonstrate Australian citizenship.
- Demonstrate a minimum of five years of technical ICT experience, with at least two years of information

security experience on systems using the ISM and supporting publications.

- Show evidence of relevant ICT and auditing qualifications.
- Complete an IRAP new starter training course.
- Undertake the ASD new starter examination.

In turn, *CSPs hire IRAP Assessors to assesses the CSP's cloud services and to produce a CSP Security Fundamentals and Cloud Services Report*. The CSP may, in turn, submit the report to procuring agencies interested in using their services.⁶⁸ ICT professionals approved to serve as IRAP Assessors are listed in the *ACSC Registrar*.⁶⁹ As of July 2022, there were approximately 200 IRAP Assessors in Australia.

Australian public sector organizations (or "procuring agencies") are responsible for assessing their own cloud service needs and security requirements to inform procurement of a cloud service. Some procuring agencies, state and local governments, government owned corporations and universities, may not require IRAP-assessed cloud services if they have lower security requirements. Those procuring agencies that do require IRAP-assessed cloud services refer to the *CSP Security Fundamentals and Cloud Services Reports* produced by IRAPs as a basis for their own risk assessments to determine if the cloud service meets their security needs. The procuring agency's Authorizing Officer (AO) is the final decision-maker on whether or not a commercial cloud service meets the agency's security requirements and does not exceed its risk tolerances.

Coordination Among Organizations

DTA and ACSC are the primary organizations responsible for policy guidance of government cloud security. DTA's *Secure Cloud Strategy* outlines a decentralized approach for cloud security. Agencies are expected to develop their own cloud strategies and plans using the *Secure Cloud Strategy* as a foundation, with support from various ACSC guidance documents, such as the *Anatomy of a Cloud Assessment and Authorisation*.

The DTA also hosts a Cloud Marketplace⁷⁰ from which procuring agencies can find and engage CSPs that have cloud services that may fit their needs. The Cloud Marketplace includes over 300 CSPs. The Cloud Marketplace also includes cloud services that are not IRAP-assessed.

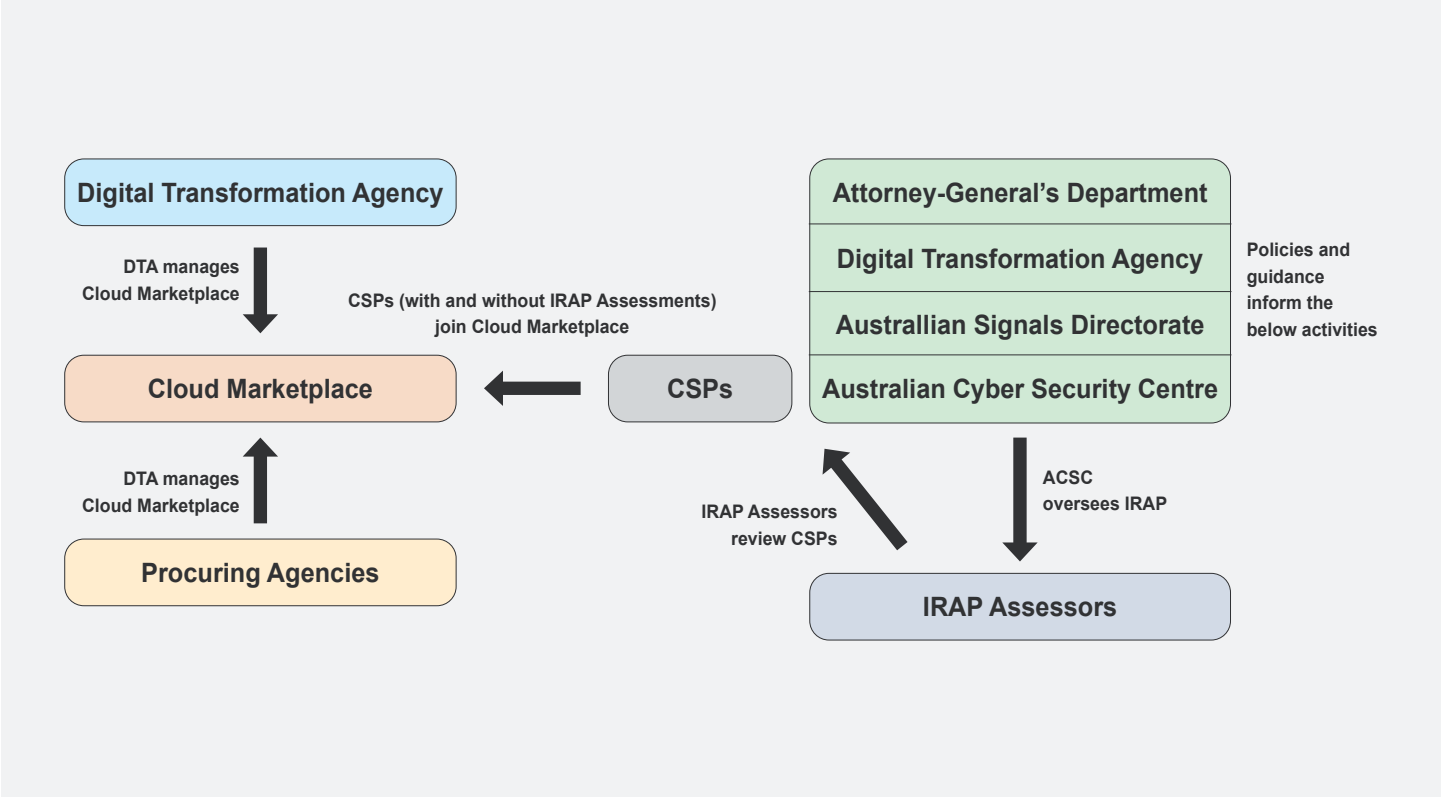
CSPs interested in entering into Australia’s public sector market should consider hiring an IRAP Assessor to review its company and suite of cloud services. The resulting *CSP Security Fundamentals and Cloud Services Report* can be shared with any interested procuring agency. Many procuring agencies request the IRAP assessment report when issuing a Request for Quote (RFQ) on the Cloud Marketplace.

Ultimately, each procuring agency is responsible for developing its own cloud procurement security strategy tailored to its value case, workforce plan, best-fit cloud model, and service readiness assessment. An agency may review an IRAP’s *CSP Security Fundamentals and*

Cloud Services Report to determine whether the CSP and its related cloud services meet the agency’s risk profile. Other considerations in this decision-making process include a cloud service’s integration with the agency’s existing ICT system, achieving Value for Money, environmental considerations, and data residency. **The procuring agency and CSP are also responsible for continuously monitoring and assurance of the cloud service.** For example, CSPs must hire an IRAP Assessor to conduct a reassessment every 24 months.

Figure A2.1 presents the relationships and coordination mechanisms described.

> > >
FIGURE A2.1 - Notional Framework of Australia’s Institutional Mechanisms for Secure Cloud Procurements



Source: World Bank.

3. Data Classification and Security Framework

The Australian government has a robust data classification system for government data/information. It also has its own unique security framework, the *Information Security Manual (ISM)*. The government has published numerous guidance

documents outlining the process to procure secure cloud service for Australian public agencies. These documents enact the Australian government’s policies on data classification, security controls, and preapproval processes.

Data Classification

The *PSPF* outlines the Australian government’s data classification system, based upon Confidentiality, Integrity, and Availability (CIA) requirements, as detailed in Figure A2.2 below.

> > >

FIGURE A2.2 - Australian Government’s Data Classification System ([PSPF Policy 08 – Sensitive and classified information](#))

		Sensitive information		Security classified information		
	UNOFFICIAL	OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise of information confidentiality would be expected to cause ➡	No damage. This information does not form part of official duty.	No or insignificant damage. This is the majority of routine information.	Limited damage to an individual, organisation or government generally if compromised.	Damage to the national interest, organisations or individuals.	Serious damage to the national interest, organisations or individuals.	Exceptionally grave damage to the national interest, organisations or individuals.

Source: [Protectivesecurity.gov.au](https://protectivesecurity.gov.au).

Unclassified information is divided into three subcategories: UNOFFICIAL, OFFICIAL, and OFFICIAL: Sensitive.

- The UNOFFICIAL category includes information with no impact on the agency’s activities and would not cause the agency any damage in the event of an attack.
- The OFFICIAL category includes information that has a low-to-medium business impact and would result in no damage, insignificant damage, or limited damage. This information includes routine information or is limited to an individual or organization.
- The OFFICIAL: Sensitive category includes Official information that would have low-to-medium impact with limited damage on an agency.

Classified information is also divided into three subcategories: PROTECTED, SECRET, and TOP SECRET.

- The PROTECTED category includes information with a high impact on agency operations and a risk of damage to the national interest, organization in question, or an individual.
- The SECRET category includes information with an extreme impact on organization operations, in which a compromise would result in serious damage to the national interest, the organization in question, or an individual.
- The TOP SECRET category includes information with a catastrophic impact on organization operations, which would cause exceptionally grave damage to the national interest, the organization in question, or an individual.



The Australian government has established conditions for the types of data that can be handled by CSPs. The government allows CSPs without security clearances to store, process, and communicate data at or below the OFFICIAL: Sensitive level. CSPs that store, process, or communicate data classified at and above the PROTECTED level are required to have personnel who hold security clearances at the commensurate level. The government may also allow employees of CSPs temporary access to information at or below the SECRET level for personnel without a security clearance on a case-by-case basis. These types of access opportunities are tightly supervised by Australian government entities.

Data Residency

Australia does not have any explicit law prohibiting the storing or processing of Australian data overseas. But ACSC “recommends cloud consumers use CSPs and cloud services located in Australia for handling their sensitive and security-classified information.”⁷¹ The ACSC further notes that, “CSPs that are owned, based and solely operated in Australia are more likely to align to Australian standards and legal obligations, and this reduces the risk of any data type being transmitted outside of Australia.”⁷² Again, however, the government only advises (but does not require) procuring agencies to keep more sensitive data within Australian boundaries.

In addition, the DTA’s Hosting Certification Framework (HCF) outlines the certification process for CSPs to host sensitive or classified data.⁷³ Procuring agencies are required to use HCF-certified services and associated infrastructure to handle data at the OFFICIAL: Sensitive and PROTECTED classification level. There are three levels under the HCF.⁷⁴

1. **Strategic level** represents the highest level of assurance and is only available to CSPs that allow the government to specify ownership and control conditions. A Certified Strategic CSP offers additional protections, including increased security controls, compared to a Certified Assured CSP.
2. **Assured level** provides safeguards against change of ownership or control through financial penalties that are aimed at minimizing the transition costs should a CSP alter its profile. Government customers with a low-risk profile handling sensitive data, which has been deemed by the government customer to not need additional security protections, may seek the services of a Certified Assured CSP.
3. **Uncertified level** offers minimal protections to government. Government customers may use the services of an Uncertified CSP to host nonsensitive data or where their internal risk assessment determines it appropriate.

Security Controls

ACSC’s cloud security control framework is outlined in the ISM and its associated CSCM. The ISM organizes its security controls under four categories: **govern, protect, detect, and respond**. These controls are used to inform procuring agency security risk management plans for their selected cloud service. The ISM draws the foundation of its guidance from NIST’s Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations: A System Lifestyle Approach for Security and Privacy*.⁷⁵

TABLE A2.1 - ISM Security Control Principles⁷⁶

Category	Principle
Govern	G1: Chief Information Security Officer provides leadership and oversight of cyber security.
	G2: The identity and value of systems, applications, and data is determined and documented.
	G3: Confidentiality, integrity, and availability requirements for systems are determined and documented.
	G4: Security risk management processes are embedded in organizational risk management.
	G5: Security risks are identified, documented, managed, and accepted before systems are authorized and continuously monitored.
Protect	P1: Systems are designed, deployed, maintained, and decommissioned according to their value, confidentiality, integrity, and availability.
	P2: Systems are delivered and supported by trusted suppliers.
	P3: Systems are configured to reduce their attack surface.
	P4: Systems are administered in a secure and accountable manner.
	P5: Security vulnerabilities in systems are identified and mitigated in a timely manner.
	P6: Only trusted and supported operating systems, applications, and computer code can execute on systems.
	P7: Data is encrypted at rest and in transit between different systems.
	P8: Data communicated between different systems is controlled and inspectable.
	P9: Data applications and configuration settings are backed up in a secure and proven manner on a regular basis.
	P10: Only trusted and vetted personnel are granted access to systems, applications, and data.
	P11: Personnel are granted the minimum access to systems, applications, and data required for their duties.
	P12: Multiple methods are used to identify and authenticate personnel to systems, applications, and data.
	P13: Personnel are provided with ongoing cyber security awareness training.
	P14: Physical access to systems, supporting infrastructure, and facilities is restricted to authorized personnel.
Detect	D1: Event logs are collected and analyzed in a timely manner to detect cyber security threats.
	D2: Cyber security events are analyzed in a timely manner to identify cyber security incidents.

Table A2.1 continued

Category	Principle
Respond	R1: Cyber security incidents are reported internally and externally to relevant bodies in a timely manner.
	R2: Cyber security incidents are contained, eradicated, and recovered from in a timely manner.
	R3: Business continuity and disaster recovery plans are enacted when required.

Source: [Cyber Security Principles | Cyber.gov.au](https://www.cyber.gov.au/cyber-security-principles).

The CSCM complements the ISM by providing guidance on the scoping of cloud security assessments by classification level. For example:

- Cloud services using OFFICIAL (including OFFICIAL: Sensitive) data include 726 security controls
- Cloud services using PROTECTED data include 726 security controls
- Cloud services using SECRET include 783 security controls
- Cloud services using TOP SECRET include 791 security controls

Ultimately, the CSCM is considered guidance for IRAP Assessors, which are responsible for determining on a case-by-case basis the relevant ISM security controls to be included in an assessment.⁷⁷ IRAP assessors can provide security assessments for CSPs at or below the SECRET level.

ISM and its corresponding CSCM are the sole standard against which the IRAP Assessor should review a CSP, although international frameworks may be useful references for the IRAP Assessor. Indeed, the ACSC notes: “International standards and certifications vary in the level of assurance they provide, and none exist that completely align to the security controls in the ISM. For this reason, when assessing a CSP and its cloud services for use by cloud consumers, there is no substitute for a CSP being assessed by an IRAP assessor against the security controls in the ISM.”⁷⁸

Preapproval Process

ACSC’s *Anatomy of a Cloud Assessment and Authorisation* outlines the preapproval process for cloud procurements under the Cloud Security Strategy.

The Australian government outlines a standard methodology by which an IRAP Assessor must assess a

CSP and its cloud services. An IRAP Assessor must take several steps to prepare for the assessment process, such as:

- Confirm the intended classification of the data to be handled by the CSP and its cloud services.
- Identify the ISM security controls that are in scope of the data classification level.
- Take any tailoring actions to the ISM security controls to ensure organizational risk will be mitigated.

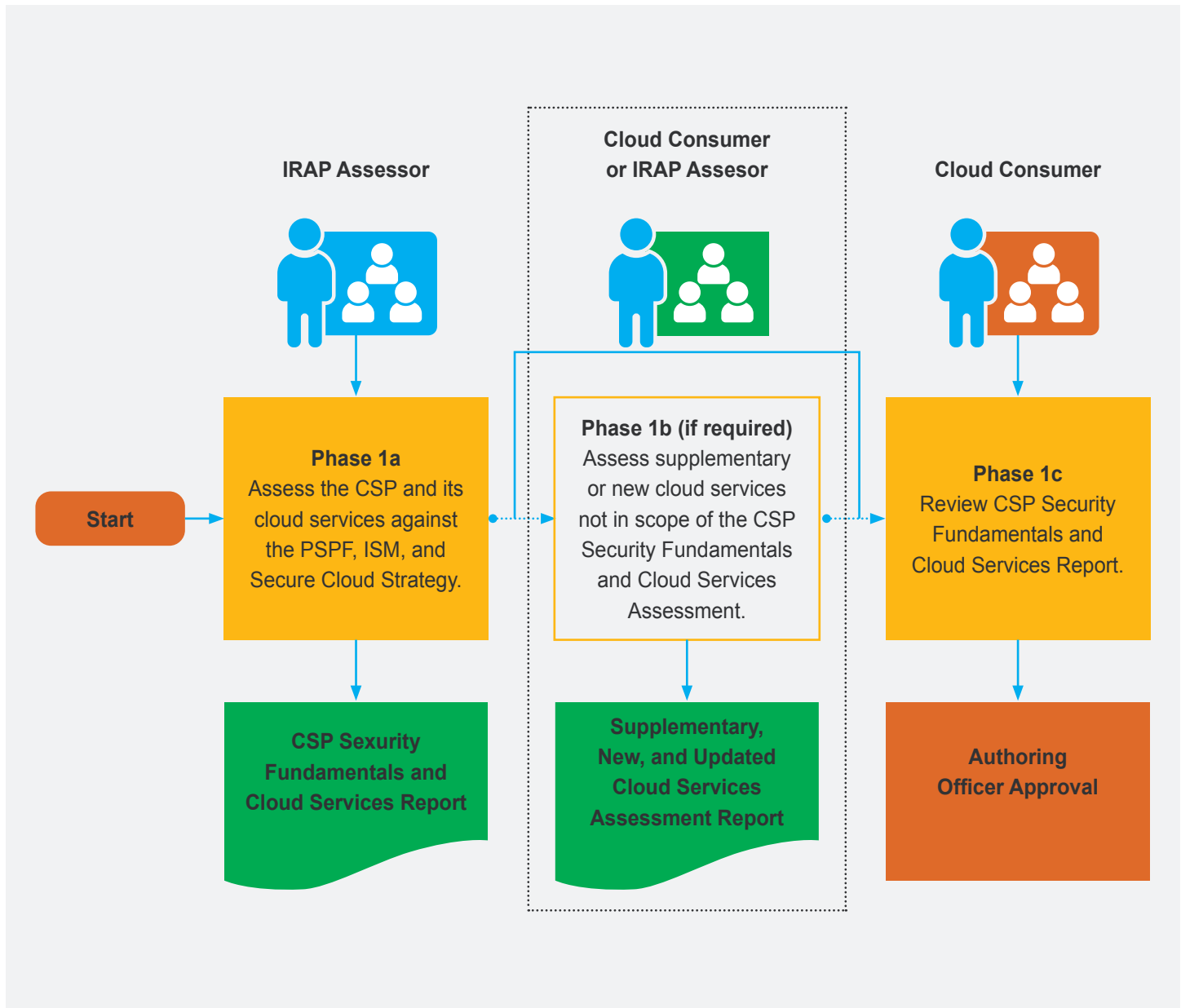
In turn, the Cloud Assessment and Authorization process consists of two phases:

PHASE 1: CSP security fundamentals and cloud services assessment.

In Phase 1A, the IRAP Assessor reviews the security of the company and each of its cloud services against the applicable ISM security controls. The IRAP Assessor produces CSP Security Fundamentals and Cloud Services Report.⁷⁹ During the assessment, an IRAP Assessor may accept some inherited controls of CSPs and cloud services that have already undergone an IRAP assessment. For example, a CSP offering SaaS may inherit security controls from another CSP’s IaaS upon which it is built.

In Phase 1B, an IRAP Assessor or the procuring agency itself must assess a different, new, or significant change to a cloud service that was not assessed in the original Phase 1A. These are typically narrower, less-intensive, and less time-consuming assessments.

In Phase 1C, the CSP may send the IRAP Assessor’s CSP Security Fundamentals and Cloud Services Report to any interested procuring agency for its review. The procuring agency’s AO determines if the cloud service meets its security requirements and risk tolerance.

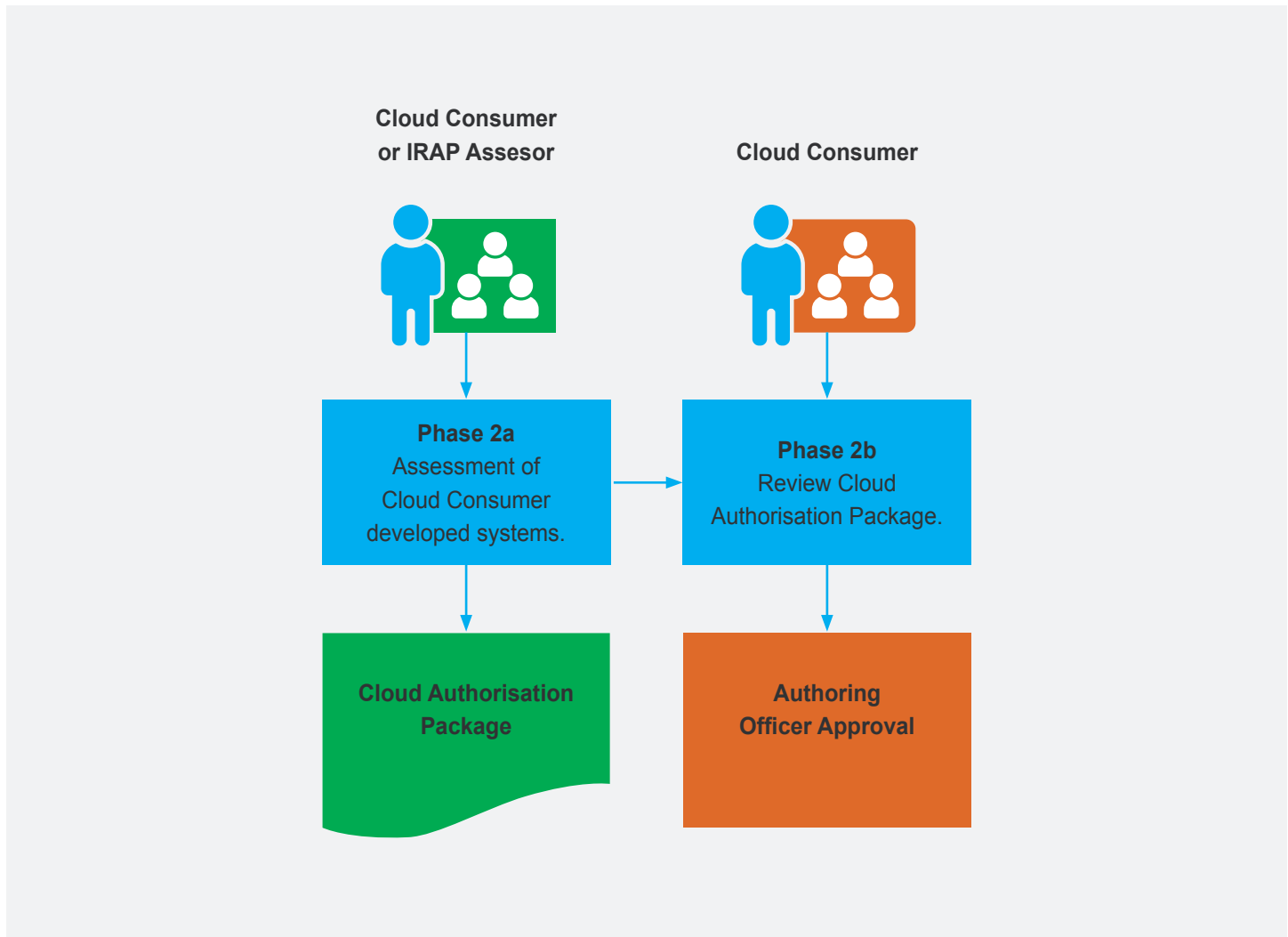
FIGURE A2.3 - Phase 1 of the Cloud Assessment Process for Australian Procuring Agencies

Source: [Anatomy of a Cloud Assessment and Authorisation | Cyber.gov.au](https://www.cyber.gov.au/Anatomy-of-a-Cloud-Assessment-and-Authorisation).

PHASE 2: Cloud consumer systems assessment and authorization

In Phase 2A, the procuring agency or IRAP Assessor evaluates any cloud systems developed by the agency to ensure they meet the agency's security requirements and risk tolerance. This process underscores the shared responsibility between the procuring agency and the CSP on ensuring cybersecurity of the cloud environment.

In Phase 2B, the procuring agency must provide to the AO an "Authorization Package" including the CSP Security Fundamentals and Cloud Services Report, the Phase 2A report, and any other supplemental information. The AO makes the final decision on whether or not to approve the cloud service.

FIGURE A2.4 - Phase 2 of the Cloud Assessment Process for Australian Procuring Agencies

Source: [Anatomy of a Cloud Assessment and Authorisation. Cyber.gov.au.](https://www.cyber.gov.au/~/media/Assets/Cloud%20Assessment%20and%20Authorisation.pdf)

ALL PHASES: Continuous Monitoring. The procuring agency and CSP must conduct continuous monitoring and assurance to provide ongoing awareness of evolving information security risks, vulnerabilities, and threats. CSPs must keep the procuring agencies informed of changes to their security fundamentals that impact their security baseline and that of the procuring agency's systems. Moreover, the CSP and its cloud services must undergo reassessments by an IRAP Assessor every 24 months.

Reuse of IRAP Assessments. A CSP can make its CSP Security Fundamentals and Cloud Services Report available

to any procuring agency that requests it. Procuring agencies that perform their own supplementary, new, and updated cloud services assessments under Phase 1B of the cloud security guidance are also encouraged to share these reports with other procuring agencies and the CSP. These procedures allow for the reuse of assessment reports, thus streamlining and standardizing the preapproval process for procuring cloud services. Moreover, the standardized use of the CSP Security Fundamentals and Cloud Services Report allows procuring agencies to compare CSPs more easily to one another and determine which CSP best meets their needs.

4. Procurement Arrangements

ACSC's *Anatomy of a Cloud Assessment and Authorisation* outlines the requirements for cloud procurements under the *Cloud Security Strategy*.

The DTA's Cloud Marketplace offers a centralized location for procuring agencies to find CSPs and their cloud services.⁸⁰ The Cloud Marketplace includes more than 300 CSPs—some IRAP-assessed and others not. The Cloud Marketplace is a panel arrangement: suppliers under the arrangement are appointed to supply services for a set period of time under agreed terms and conditions. CSPs on the Cloud Marketplace must make a maximum and minimum for the price range available to buyers in the online catalogue.

DTA adds CSPs to its Cloud Marketplace through periodic “market refreshes” approximately every 12 to 18 months for the life of the marketplace, which is three years in its initial term (2021-2024), with the possibility of two 1-year extensions. During a refresh, DTA releases a Request for Tender on the Australian Government's tendering platform, Austender. CSPs may use this tender process to join and add their cloud services to the Cloud Marketplace. They are required to submit a cloud service to be evaluated by DTA, which determines if the service should be added onto the Cloud Marketplace. The DTA's considerations for additions to the Cloud Marketplace include technical and security criteria, company structure and management, financial considerations, and whether the proposed cloud service is deemed to be value-for-money. In addition to the refresh process, CSPs on the Cloud Marketplace may also add other cloud services to their catalogue of offerings.

The Cloud Marketplace is a procurement mechanism. As such, each procuring agency seeking a cloud service must undergo a competitive bidding process under an RFQ. There is an expectation that the competitive bidding helps to achieve the best value for money for the procuring agency. A CSP may undercut its own catalogue prices on the Cloud Marketplace (even below its published lowest price) during a bidding. But a CSP may not charge more than their maximum price listed on the Cloud Marketplace.

During the procuring agency's evaluation of vendor responses to its RFQ, the agency must take into consideration several factors such as:

- Security requirements, including an IRAP assessment, if needed.
- Achieving value-for-money throughout the life of a procurement is a core component of the Australia's Procurement Rules for its procuring agencies. Total cost of ownership consideration is included in the value-for-money perspective.
- Climate change impacts.
- Benefits to the Australian economy (for relevant procurements above \$4 million).

Once a procuring agency selects its vendor, it creates a contract under the Cloud Marketplace panel arrangement. DTA offers a contract template for procuring agencies entering into a procurement with a CSP on the Cloud Marketplace Most agencies buy subscription-based units over a period, up to three years. In addition, procuring agencies must pay a two percent buyer Central Administration Fee (CAF) for contracts valued at AU\$25,000 or more. The CAF is capped at AU\$200,000 for contracts with a value greater than AU\$10 million.

Cloud services purchased on the marketplace are suitable for simple procurements of Commercial off-the-shelf (COTS) cloud solutions, along with more complex cloud solutions.

In addition, for procuring agencies choosing not to use the Cloud Marketplace, as the Cloud Marketplace is not a mandatory procurement mechanism, DTA also provides a Cloud Sourcing Contract Template to provide procuring agencies a model contract with a CSP, along with a Cloud Services Minimum Terms Template to help clarify minimum terms between the two parties.⁸¹



Annex 3. UK's Digital Marketplace and G-Cloud Framework

1. Brief History and Background of UK's Cloud Security Governance

Since 2013, the UK government has promoted the public sector adoption of cloud services through its *Cloud First Policy*, which stipulates that when procuring new or existing services, procuring agencies should consider and fully evaluate potential cloud solutions first before considering any other option.⁸² The UK government also clarifies that cloud first prioritizes public cloud solutions, rather than community, hybrid, or private deployment models.⁸³

To promote ICT offerings, the UK government established the Digital Marketplace⁸⁴ in 2014 to be a centralized catalogue of approved ICT services including cloud for UK procuring agencies. Administered by the Crown Commercial Service (CCS), the Digital Marketplace carries over 31,000 cloud services that can be procured using the G-Cloud Framework, a mechanism that eases the procurement process for procuring agencies.⁸⁵ Vendors must meet certain minimum cybersecurity and data privacy requirements to be registered onto the Digital Marketplace.

In addition to the Digital Marketplace, CCS promotes a common cloud procurement process across the UK public sector through its Cloud Compute (RM6111) Framework.⁸⁶ There are nine hyperscalers on the Cloud Compute Framework: AWS, Fordway, Frontier Technology LTD, Google Cloud, IBM, Microsoft, Oracle, UKCloud, UKFast. The Cloud Compute Framework offers procuring agencies the opportunity to directly contract with hyperscalers. Procuring agencies may issue direct award or competitive bids under the Cloud Compute Framework. Overall, this Framework aims to allow procuring agencies to save time and cost when procuring hyperscaler services such as cloud storage and hosting.

Procuring agencies are encouraged to follow the National Cyber Security Centre's (NCSC) *Cloud Security Guidance* when seeking to procure a cloud service.⁸⁷ Originally published in 2018, the Guidance offers insights into how organizations can choose cloud services and also outlines 14 Cloud Security Principles to help organizations implement and maintain sound cloud security over the lifetime of a cloud service procurement. The *Cloud Security Guidance* is complemented by various UK government publications, including the *Security Policy Framework*,⁸⁸ the *Minimum Cyber Security Standard*,⁸⁹ and the *Risk Management Guidance*.⁹⁰

In 2015, the UK's Government Digital Service (GDS) established the "GOV.UK PaaS," a cloud hosting platform for public sector digital services for use by both public and non-public sector organizations running public sector digital services.⁹¹ However, GDS announced in July 2022 that it would discontinue GOV.UK PaaS, partly because the platform could not keep up with the service offerings of major public cloud providers such as AWS and Azure.

2. Institutional Coordination Mechanisms

The UK government has numerous organizations that promote its cloud first policy and associated preapproval and procurement process.

Key Organizations

GDS under the UK Cabinet Office that is responsible for leading the UK government's digital transformation. In this capacity, GDS develops and maintains the UK government's IT platforms, products, and services. GDS developed the Digital Marketplace, which is now managed by the CCS.

CCS under the UK Cabinet Office that facilitates procurements of commercial services by the public sector. In this capacity, CCS administers the Digital Marketplace and negotiates the Cloud Compute Framework on behalf of the UK government.

The Central Digital and Data Office (CDDO) under the UK Cabinet Office leads digital, data, and technology functions for the UK government. The CDDO promotes various cloud and security policies for procuring agencies, such as the *Technology Code of Practice* (TCoP), which outlines the cloud first policy and offers guidance on securing government technology programs.

NCSC is the primary cybersecurity agency of the UK government, working collaboratively with domestic and international partners to promote cybersecurity. NCSC routinely publishes various cybersecurity guidance documents to inform procuring agencies and others on cybersecurity best practices. NCSC also partners with the IASME Consortium⁹² to facilitate the "Cyber Essentials" certification,⁹³ a recognized UK government cybersecurity standard certification.

UK public sector organizations or procuring agencies procure the cloud services from the Digital Marketplace or

the Cloud Compute Framework. These entities are ultimately responsible for working with CSPs to ensure the security of the cloud service across the lifetime of its procurement.

Coordination Among Organizations

As the primary commercial procurement arm of the UK government, CCS administers the Digital Marketplace. CCS receives technical support from other UK government organizations, such as the GDS and CDDO, to fulfill these responsibilities. CCS and its partners support procuring agencies in procuring commercial cloud services through on-demand support and published guidance. CCS also

negotiates the Cloud Compute Framework with hyperscalers. Procuring agencies may purchase cloud services through this prearranged Framework.

The NCSC offers guidance and advice on cloud security to procuring agencies. In this capacity, NCSC serves an advisory role, as opposed to a regulatory or oversight role for the cloud security of procuring agencies. In addition to its 14 Cloud Security Principles (Table A3.1), NCSC also offers a lightweight approach to cloud security, which provides guidance for agencies seeking to conduct a “rapid but reliable” assessment of cloud services that process less-sensitive data.

> > >

TABLE A3.1 - NCSC’s 14 Cloud Security Principles

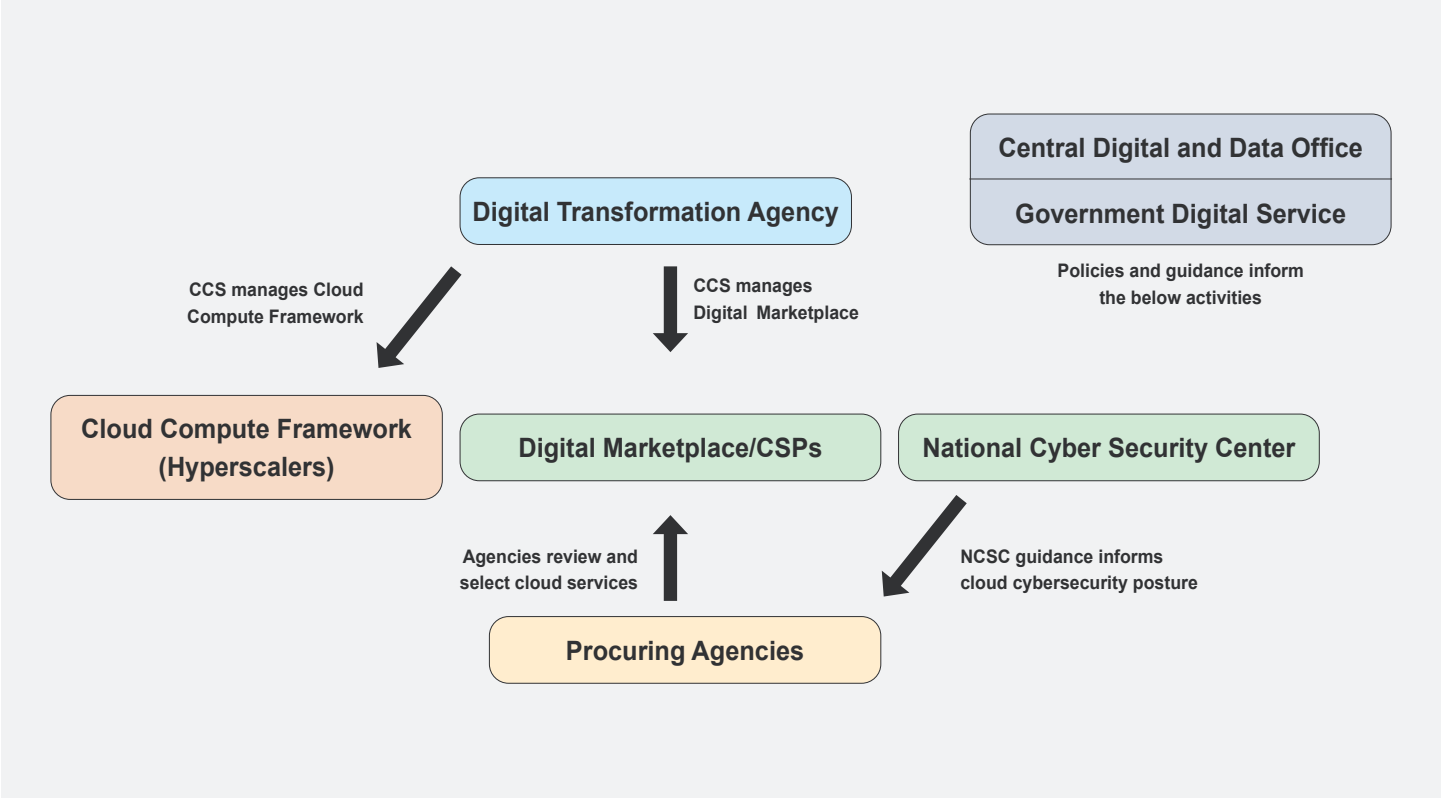
Principle 1	Data in transit protection
Principle 2	Asset protection and resilience
Principle 3	Separation between customers
Principle 4	Governance framework
Principle 5	Operations security
Principle 6	Personnel security
Principle 7	Secure development
Principle 8	Supply chain security
Principle 9	Secure user management
Principle 10	Identify and authentication
Principle 11	External interface protection
Principle 12	Secure service administration
Principle 13	Audit information and alerting for customers
Principle 14	Secure use of the service

Source: NCSC, UK.

Ultimately, each procuring agency is responsible for leveraging NCSC’s guidance to help ensure adequate cybersecurity risk management when procuring a cloud service.

> > >

FIGURE A3.1 - Notional Framework of the UK’s Institutional Mechanisms for Secure Cloud Procurements



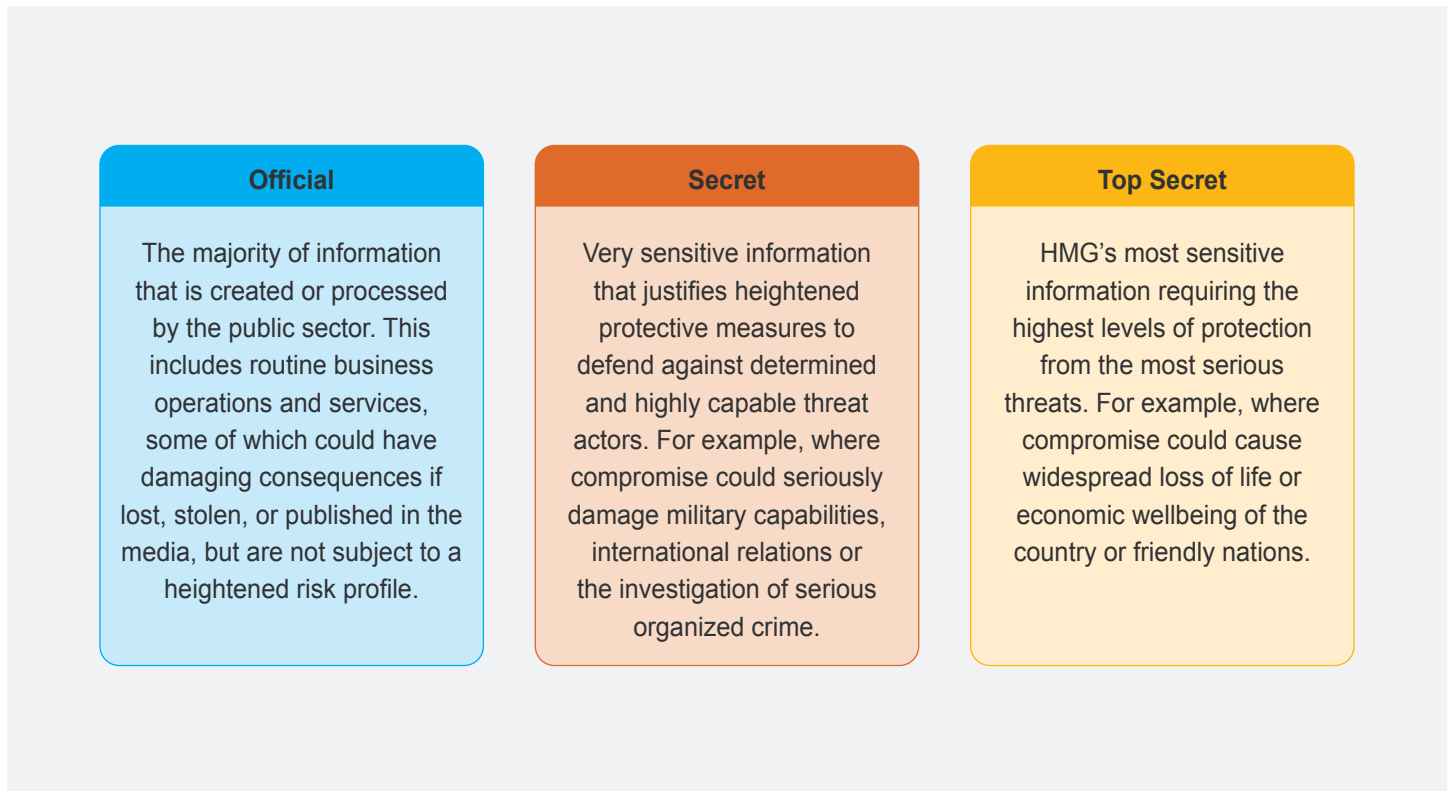
Source: World Bank.

3. Data Classification and Security Framework

The UK government has a data classification policy for UK government data. NCSC also offers guidance on securing cloud systems but does not include any mandatory security control framework for procuring agencies seeking to purchase cloud services.

Data Classification

The UK Cabinet Office’s *Government Security Classifications* (May 2018) is the official data classification policy of the UK government. It promotes a three-tiered data classification system: OFFICIAL; SECRET; AND TOP SECRET.

FIGURE A3.2 - The UK's Data Classification System

Source: [May-2018_Government-Security-Classifications-2.pdf, publishing.service.gov.uk](#).

Unlike other case studies, the UK bases its classification system only on confidentiality requirements. The UK government states that a high integrity or availability requirements do not lead to a higher data classification within its system. **Within this general framework, the UK government can provide more specific descriptors to its data.** For example, organizations may apply a descriptor to an “OFFICIAL” marking to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access. In these cases, the UK government may classify data as “OFFICIAL-SENSITIVE [DESCRIPTOR]”. Some examples include:

- OFFICIAL-SENSITIVE COMMERCIAL refers to market-sensitivity information that may be damaging to HMG or to a commercial partner if improperly accessed.

- OFFICIAL-LOCALLY SENSITIVE or LOCSEN refers to sensitive information that locally engaged staff overseas cannot access.
- OFFICIAL-SENSITIVE PERSONAL refers to particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences.

The vast majority of public sector data is considered OFFICIAL. In fact, the UK government has estimated that the official classification covers up to 90 percent of all public sector business.⁹⁴

Data Residency

The UK government does not have any strict data residency requirements for cloud services. Indeed, according to the CDDO: “There is no government policy which directly prevents departments or services from storing cloud-based data in any specific country, however you need to consider the implications of where you host your data.”⁹⁵ As such, each public sector agency is expected to make a risk-based judgment on whether it can allow transfer of government data outside the UK, based upon the sensitivity of its data and information.

Security Controls

The UK government does not subscribe to one type of cybersecurity standard or set of security controls when procuring cloud services. For example, the UK government does not mandate a specific set of security controls or certifications necessary to be added to the Digital Marketplace. The G-Cloud Framework requires suppliers to self-declare various cybersecurity-related information and accept some cybersecurity conditions in order to be added to the Digital Marketplace – see **Section 4** on Procurement Arrangements below. The self-declaration forms are available on the UK government’s GitHub page.⁹⁶

Moreover, the possession of third-party security certifications is considered beneficial. CSPs with security certifications such as NCSC’s *Cyber Essentials* or the *ISO/IEC 27000* family may be considered more trustworthy for UK procuring agencies. In addition, NCSC encourages procuring agencies to refer to its **14 Cloud Security Principles** when choosing a cloud service to meet security needs. Organizations can also use them as guidance on how to securely configure their own cloud systems.

Furthermore, the UK government’s *Service Manual Guidance on Securing Information for Government Services*⁹⁷ offers guidance to public agencies on how to secure OFFICIAL data. The *Service Manual* guides organizations on how to develop security protocols for services that use OFFICIAL data and information.⁹⁸ For example, the *Service Manual* calls on government teams to consider the CIA, non-repudiation, and privacy considerations of its data and information when developing security plans. The *Service Manual* also refers to additional resources that can be consulted by procuring agencies to manage security risks:

- *Securing Your Cloud Environment*.⁹⁹
- *Security Policy Framework*.¹⁰⁰

- *Risk Management Guidance*.¹⁰¹
- *Secure Development and Deployment Guidance*.¹⁰²

Preapproval Process

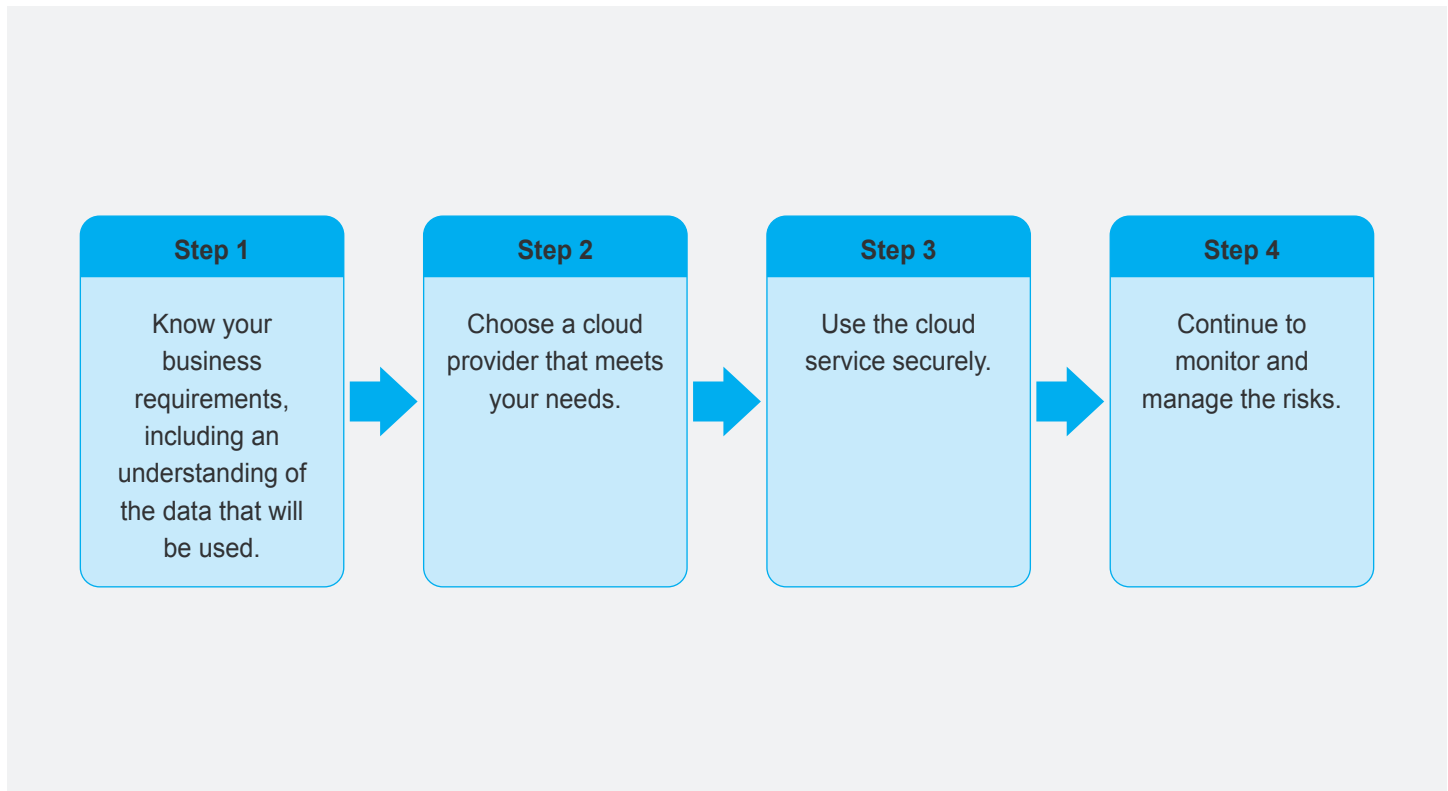
Procuring agencies may buy commercial cloud services through the Digital Marketplace or the Cloud Compute Framework. Each option includes certain requirements to promote the cyber risk management of the procuring agency.

Digital Marketplace. The first step in assessing and preapproving the cloud security of a cloud service is registration to the Digital Marketplace. CSPs in the Digital Marketplace must agree to the terms of the G-Cloud Framework agreement,¹⁰³ a contractual agreement between the CSP and CCS. The G-Cloud Framework is updated every two years. CSPs must transition to the updated G-Cloud Framework every two years, although there is some flexibility for extensions on this timeline.

The G-Cloud Framework requires suppliers to issue a self-declaration of conformity to various cybersecurity and data privacy-related information, such as any security certifications and its efforts to protect the integrity, confidentiality, and security of the procuring agency data held or used by the CSP.¹⁰⁴ The G-Cloud Framework also requires each to self-declare that it accepts the following conditions:

- The CSP must maintain IT security that follows good industry practice to prevent unauthorized access to government data.
- The CSP must immediately notify CCS and its procuring agency of a security and/or personal data breach and take all necessary steps to recover from and investigate the breach.
- The CSP must comply with UK’s data protection legislation which requires organizations to meet various requirements such as the EU’s General Data Protection Regulations (GDPR) to help ensure data privacy protections.
- The CSP must permit CCS or a third-party auditor under CCS’s direction to conduct an audit of its cybersecurity posture, if requested.

NCSC also outlines a four-step process¹⁰⁵ for procuring agencies to securely procure public cloud services from the Digital Marketplace:

FIGURE A3.3 - NCSC's Four-Step Process for Procuring Public Cloud Services

Source: NCSC.

Cloud Compute Framework: Hyperscalers listed under the Cloud Compute Framework also agree to baseline cybersecurity requirements under the terms of the Framework.¹⁰⁶

4. Procurement Arrangements

CCS's Digital Marketplace and the Cloud Compute Framework provide centralized locations for procuring cloud services. Within this context, each individual agency is ultimately responsible for ensuring adequate cybersecurity when procuring and using cloud services.

Digital Marketplace: The Digital Marketplace provides procuring agencies the option to buy pay-as-you-go cloud services on government-approved, short-term contracts through CCS's eSourcing tool. Each service includes pricing information for potential buyers. The Digital Marketplace offers three categories or lots of cloud services for UK procuring agencies:

1. **Cloud Hosting.** PaaS or IaaS services for processing and storing data, running software, or networking—for example, content delivery networks or load balancing services.
2. **Cloud Software.** Applications (SaaS) that are accessed over the internet and hosted in the cloud, such as accounting tools or customer service management software.
3. **Cloud Support.** Services to help procuring agencies to set up and maintain their cloud software or hosting services—for example, migration services or ongoing support.

In the procurement phase, procuring agencies can purchase a cloud service on the Digital Marketplace in one of two ways:

- *First*, if only one supplier in the Digital Marketplace meets its needs or requirements, then the procuring agencies can issue a direct award by issuing a Call-Off Contract to that G-Cloud supplier. CCS provides procuring agencies a standardized template for the G-Cloud Call-Off Contracts.¹⁰⁷

- *Second*, if the procuring agency has multiple suppliers that meet its needs or requirements, it can either select the lowest-priced cloud service or conduct a more thorough review of the best value purchase based upon numerous factors, including total cost of ownership, technical merit and functional fit, and service management.¹⁰⁸ The procuring agency must simply provide justification for which procurement method it uses – lowest-priced versus best value. Ultimately, the procuring agency will enter into a Call-Off Contract with its selected cloud service.

The Digital Marketplace also features built-in protection against vendor lock-in. For example, the maximum length of a G-Cloud contract from the Digital Marketplace is normally 24 months. Procuring agencies have the option to annually extend the contract by one year and then another year to a maximum of four years, if desired. The CDDO also offers guidance on its website for organizations on how to manage lock-in in the cloud by ensuring the ease and affordability of moving a system and data from one CSP to another (a concept called “portability”).¹⁰⁹

The UK government has implemented several policies to promote continuous monitoring of cloud security solutions purchased on the Digital Marketplace, including: (1) the G-Cloud Framework, which requires CSPs to provide security breach notifications; and (2) CCS, which reserves the right to conduct an audit of a CSP over the course of a contract.

The G-Cloud Framework typically offers COTS cloud solutions that can easily be integrated into an ICT environment. If, however, a procuring agency requires

special functionalities above-and-beyond COTS offerings, it may coordinate with the CCS to issue a Request for Tender for such specialized cloud services. Procuring agencies that choose to procure a CSP service outside of the G-Cloud Framework may choose longer-term contracts, if desired.

Cloud Compute Framework: Procuring agencies may work directly with hyperscalers to issue direct award of contract or undergo a competitive bid under the Cloud Compute Framework.

- *Under a direct award*, a procuring agency must develop requirements and then assess the requirements against the available hyperscaler offerings to determine which service best meets its needs. Considerations can include quality of service, pricing, and total cost of ownership. In turn, a procuring agency can issue a Call-Off Contract to the hyperscaler of its choosing.
- *Under a competitive bid*, a procuring agency must develop requirements, share the requirements with hyperscalers, and then invite them to propose a cloud solution that meets its needs and provides associated pricing details. After the procuring agency evaluates the proposals based on cost and quality, it issues a Call-Off Contract to the selected hyperscaler.

The Call-Off Contract term under this Framework is up to three years, with two possible extensions of up to 12 months each for a maximum of five years, if desired. This setup reduces the need for procuring agencies to purchase hyperscale compute services every two years through the G-Cloud Framework.



Annex 4. South Africa's Cloud Security Framework

1. Brief History and Background of South Africa's Cloud Security Governance

South Africa has one of the most advanced digital economies in Sub-Saharan Africa. The South African government has begun implementing policies to promote public sector integration of digital technologies, including cloud solutions. For example:

- In 2016, the South African Cabinet adopted the *National ICT Integrated White Paper Policy* (“*ICT White Paper*”), that promoted a vision of digital transformation for the public sector, in which ICT would be used to enhance the government's services to the public.
- In 2017, South Africa's **Department of Telecommunications and Postal Service** (DTPS) published the *National e-Government Strategy and Roadmap*.¹¹⁰ This policy document builds upon previous policies like the 2016 ICT White Paper to provide guidance on the “digital transformation of public service in South Africa into an inclusive digital society where all citizens can benefit from the opportunities offered by digital technologies to improve their quality of life.”

Currently, the South African government is deliberating on the finalization of its draft *National Data and Cloud Policy* (“*Draft Policy*”) published in April 2021 by the **Department of Communications and Digital Technologies** (DCDT).¹¹¹ The *Draft Policy* offers a whole-of-nation policy framework on data and cloud that promotes an innovative and open digital infrastructure system. **The Draft Policy, once finalized, is expected to incorporate some existing cybersecurity and privacy laws and regulations related to public sector cloud computing.** For example, the Draft Policy will likely require public cloud systems to abide by the *National Cybersecurity Policy Framework (NCPF)*. The systems will also have to comply with major data security and privacy laws including the *Electronics Communications and Transaction Act (ECTA)*, related to data and database protection; the *Protection of Personal Information Act (POPIA)*, related to data privacy; the *Protection of Information Act (PIA)*, related to disclosure of State information; and the *Minimum Information Security Standards (MISS)*, related to data classification and security policy. Moreover, the *Draft Policy* calls for data localization of certain hypersensitive data and information like defense information.

As the South African government continues to deliberate on the finalization of the *Draft Policy* that broadly pertains to the entire country, another government department, the **Department of Public Service and Administration (DPSA)**, issued the *Public Service Cloud Computing Determination and Directive* (“*Determination and Directive*”) in February 2022.¹¹² Directed toward government procuring agencies, it promotes a cloud first policy for the South African government and provides guidance to procuring agencies on the assessment, adoption, and use of cloud computing services. It also integrates existing security and privacy laws, including *POPIA* and *MISS*. Overall, the *Determination and Directive* is South Africa's primary guidance for procuring agencies seeking public cloud solutions.

2. Institutional Coordination Mechanisms

The South African government has begun to develop institutional guidance to help in facilitating secure cloud service purchases within the public sector.

Key Organizations

DPSA is responsible for the organization and administration of civil services. In this capacity, DPSA's *Determination and Directive* aims to provide a consistent policy framework across the South African public sector on cloud service procurements.

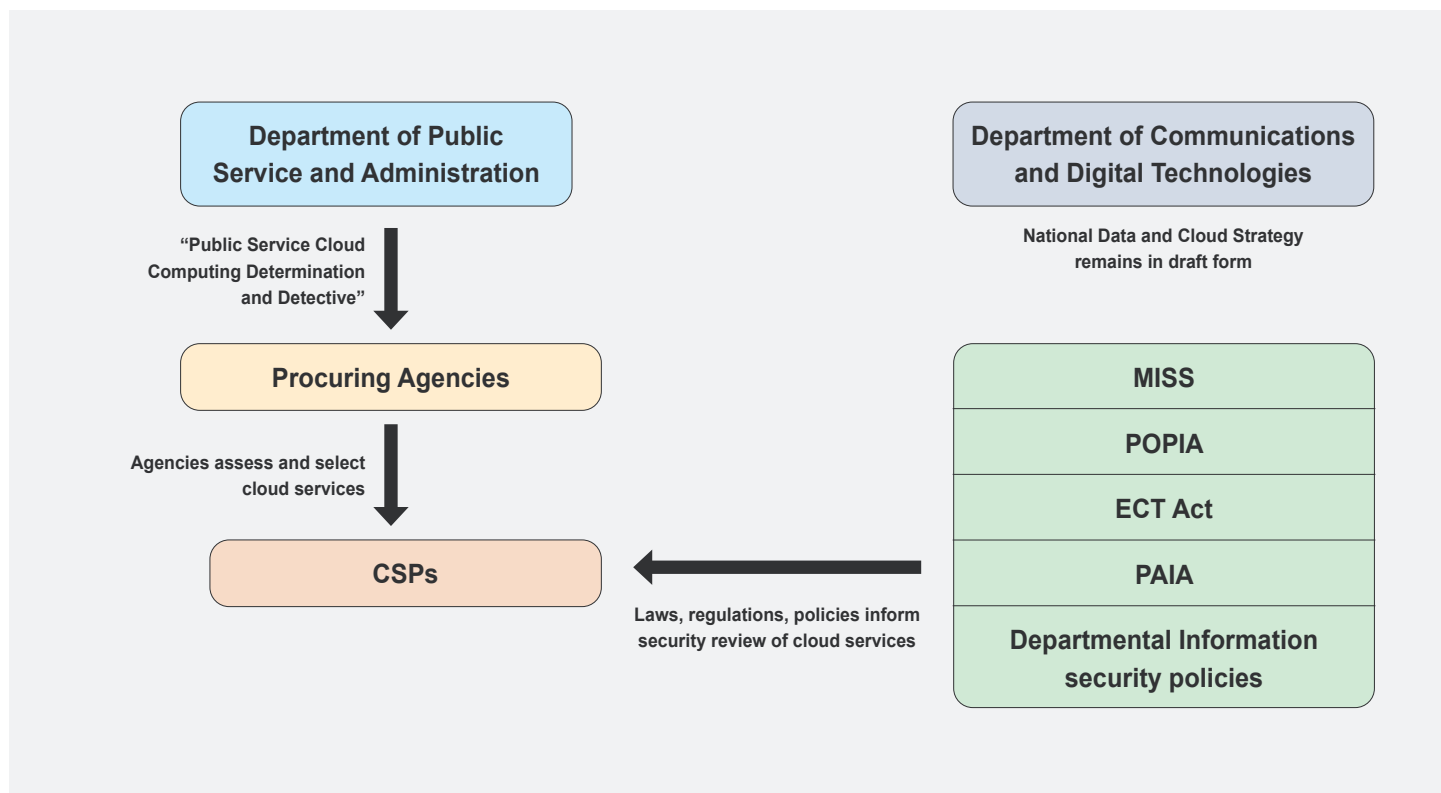
DCDT was formed in 2019 and is responsible for leading South African government efforts on digital transformation. Within DCDT, the **State Information Technology Agency (SITA)** is responsible for the provision of IT services to the government. SITA is working to build a Government Private Cloud.

South African public sector organizations or procuring agencies and their respective Heads of Department (HOD) are responsible for assessing and adopting commercial cloud services pursuant to the *Determination and Directive*.

Coordination Among Organizations

DPSA outlines the policy requirements that must be implemented by each HOD. Each HOD must follow the guidance while also abiding by any existing departmental information security policies and other security and privacy laws such as *POPIA* and *MISS*. Each Department must also submit to the DPSA an approved Business Case and Risk Assessment related to a cloud service procurement.

FIGURE A4.1 - Notional Framework of the South Africa's Institutional Mechanisms for Secure Cloud Procurements



Source: World Bank.

3. Data Classification and Security Framework

South Africa has a data classification system, but it has not yet developed a group of security controls for cloud services preapprovals.

Data Classification

South Africa's data classification system is prescribed in the *MISS*.¹¹³

Under *MISS*, South African government considers classified information as "sensitive information which in the national interest, is held by, is produced in, or is under the control of the State, or which concerns the State, and which must by reasons of its sensitive nature, be exempted from disclosure and must enjoy protection against compromise." Within this context, DPSA's *Directive on Public Service Information Security* (published June 2022)¹¹⁴ outlines a three-tier

data classification system that must be adopted by each procuring agency:

- **PUBLIC.** This information has been explicitly approved by management for release to the public.
- **CONFIDENTIAL.** This information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. The unauthorized disclosure of this information could adversely impact the department or third parties.
- **SECRET.** This classification applies to the most sensitive business information, which is intended strictly for use within a department, and restricted to those with a legitimate business need for access. The unauthorized disclosure of this information could seriously and adversely impact the department or third parties.

The data classification helps each procuring agency determine the best type of cloud service for its needs. The *Determination and Directive* stipulates that the HOD must, as far as practically possible, avoid moving data classified as Secret or Top Secret to public, hybrid, or community clouds. The *Determination and Directive* also requires that the HOD must, as far as practically possible, ensure that data that is intended for general public consumption – unclassified data – must be moved to a public cloud.

Data Residency

The *Determination and Directive* states that the HOD must ensure that data always resides within the borders of South Africa. Where this is not practically possible, the HODs must ensure compliance with section 72 of *POPIA*.

Security Controls

South Africa does not have a centralized set of security controls for the preapproval of cloud services. Instead, the *Determination and Directive* calls on each HOD to ensure that the cloud service's data security conforms to the existing departmental information security policy and that it complies with *POPIA*, the *Promotion of Access to Information Act (PAIA)*, *ECT Act*, and any other laws to which its data may be subject.

Existing Information Security Policies. Each government department is required to implement a department-specific information security policy, consistent with the *MISS* and the *DPSA's Directive on Public Service Information Security* (published June 2022).¹¹⁵

- The *MISS* and the *DPSA's Directive* are not cloud-specific, but rather they outline security requirements for security of all government agency IT systems.
- The *DPSA's Directive* offers one specific requirement on cloud security: the HOD must ensure that “thorough due diligence of the service provider’s integrity, legal agreements, physical location, and security must be conducted before deciding on a cloud service provider.”

Existing Information Security and Privacy Laws: Relevant security and privacy laws include:

- Section 72 of *POPIA* prohibits the government from transferring personal information about a data subject to a third-party in a foreign country, unless certain conditions are met – for example, the recipient is subject to data privacy requirements, the user consents, or the transfer is for the benefit of the user.¹¹⁶
- Sections 63-66 of *PAIA* outline requirements to protect the data privacy of persons, commercial information, and confidential information.¹¹⁷
- The *ECT Act* generally facilitates and regulates electronic communications and transactions. The Act includes various provisions related to cryptography, consumer protection, protection of personal information, and protection of critical databases.¹¹⁸



4. Procurement Arrangements

The *Determination and Directive* is the top guidance for South Africa's procurement guidance for secure cloud computing in the public sector. It provides instructions for the pre-procurement, procurement, and post-procurement activities of a HOD when procuring cloud services. It also

leverages other government publications for data classification and security requirements. These instructions include numerous cybersecurity and privacy requirements, as shown in Table A4.1 below:

> > >

TABLE A4.1 - Key Considerations for South African Procuring Agencies under the Determination and Directive¹¹⁹

Action	Detail
Pre-Procurement	
Data Classification	All data must be classified according to MISS. HODs should avoid moving data classified as "Secret" or "Top Secret," to the Public, Hybrid, or Community Clouds. All data intended for public consumption should be moved to Public Clouds.
Data Residency	Data should reside within the border of South Africa. If this is not practically possible, agencies should ensure compliance with Section 72 of <i>POPIA</i> .
Risk Assessment	HODs must facilitate a Risk Assessment for each cloud service they intend to utilize.
Cloud Readiness Assessment	HODs must facilitate a Cloud Readiness assessment before the decision is made to move to cloud-based computing services.
Business Case	HODs must facilitate a Business Case for a cloud service that includes the following elements: <ul style="list-style-type: none"> • Scope of cloud service required. • Budget: short-, medium-, and long term. • Total cost of ownership calculation. • Human resource skills required to support the cloud services environment. • Infrastructure required to enable the cloud service. • Intended benefit of the cloud service. • Outcome of the Risk Assessment.
Contract	HODs must conclude a valid contract with a CSP before using a cloud service. The contract must include: <ul style="list-style-type: none"> • Statement that the agency is the owner of the data, which must be maintained, backed-up and secured until returned, transferred, or deleted upon termination of the contract. • Identification of the geographic location for data storage and processing. Its location must allow for adequate governmental control over the data. • Requirement for the safe return/transfer of data should the CSP be acquired. • Specification of what will happen to the data once the contract ends; will it be returned, transferred to another CSP, or deleted.

Table A4.1 continued

Action	Detail
Contract Length	Agencies may enter into a medium-term contract – period of more than 3 years but less than 5 years – for cloud services, with allowances for early termination if needed.
Cloud Service Consumption	
Data Security	The agency must ensure security of the data on the Public Cloud is in line with existing department information security policies.
Scaling Services	HODs must oversee agency scaling of cloud service subscription levels.
Business Continuity	HODs must ensure the agency's Business Continuity plans are updated and that the agency conducts regular business continuity testing.
Data backups	HODs must ensure there is an inventory of data and applications during the contract period, and that there are mechanisms to back up the data on the Public Cloud.
Cloud Termination	
Protecting Data and Applications	The agency must ensure that all data and/or applications are transferred to a new provider, returned to the department and/or permanently deleted.

The **Determination and Directive** includes a Checklist¹²⁰ as part of its **Cloud Readiness Assessment requirement** to guide each HOD's activities during the **preprocurement, procurement, and post-procurement phases**. The checklist

reviews various pertinent questions for HODs during the cloud service lifecycle. Some key checklist items related to cybersecurity of the cloud service are detailed below.

Outlining a Security Plan	
Have you made an outline of your top security goals and concerns?	
What types of assets will be managed by the system?	
Have key assets been listed and rated based on their sensitivity?	
How assets are currently managed and how will this change when transitioned to the Cloud?	
Has the right cloud delivery model been assigned based on the assets' sensitivity?	
Has the network topology been mapped?	

Enumerating safeguards and vulnerabilities	
Have the security controls been enumerated, verified, and evaluated?	
Will all sensitive data stored in the Cloud be encrypted?	
Are remote connections to the Cloud properly encrypted?	
Have you evaluated the security risk of the server's physical location?	
Are the servers housed in guarded and locked rooms?	
Have all vulnerabilities been identified and addressed?	
Are staff properly trained on the new security protocols?	

Complying with regulations	
Have you reviewed your cloud service provider's security policies?	
Do they comply with POPI Act, PAIA, ECT Act or other regulations your data may be subject to?	
Have you drafted any contracts or agreements with your cloud service provider to bridge compliance gaps?	

Location considerations	
Where is the cloud service provider located?	
Is the location near your user base (customers or staff)?	
Will speed be adversely affected by the server's location?	
Can you visit the data center where your Cloud will be hosted?	

Overall, the *Determination and Directive* offers a succinct framework for South African public sector entities in managing cybersecurity and privacy risks when procuring cloud services.



>>>

Annex 5. Dubai's Cloud Security Risk Management Approach and Procedures

1. Brief History and Background of Dubai Cloud Adoption Strategy

Dubai, UAE has enacted several policies to promote a city-wide transition to building a globally leading digital economy overseen by a digital governance structure. Dubai established the **Dubai Digital Authority (DDA)** in 2021 to develop and oversee its policies and strategies to promote the city's digital transformation. The DDA comprises four subcomponents: **Dubai Electronic Security Center (DESC)**, **Dubai Statistics Center (DSC)**, **Dubai Data Establishment (DDE)**, and **Smart Dubai Government Establishment (SDGE)**.¹²¹

As part of its digital promotion, the **Dubai Government Excellence Program (DGEP)** has a key performance indicator (KPI) entitled **Cloud First**. Its government entities must consider cloud solutions before considering any alternatives, and public cloud solutions are preferable for systems handling open data. The KPI aims to ensure that all government entities host eligible applications on the cloud by 2025.¹²²

DESC leads the Dubai's efforts to preapprove CSPs for government procurement. DESC's *Cloud Service Provider (CSP) Security Standard* establishes requirements and guidance based upon ISO/IEC and CSA standards for CSPs seeking to work with government agencies.¹²³ The *CSP Security Standard* aligns with Dubai's *Information Security Regulation (ISR)*,¹²⁴ a technology-neutral information security standard for Dubai government entities.¹²⁵

Dubai has also mandated "Information Security Officer (ISO)" positions within each government entity to promote cybersecurity akin to the role of a Chief Information Security Officer. The ISO positions play a key role for government entities seeking to assess the security of certified CSPs against its security needs during the procurement phase.

Dubai offers **eSupply** as an online portal for CSPs and other suppliers to participate in online tenders or RFQs published by Dubai procuring agencies. Dubai also has its own cloud environment called **DubaiPulse**, a private government cloud developed by the DDA with the main aim to publish open data and to share the data between government entities. It is also equipped to host sensitive data and workloads for government entities, if needed.¹²⁶

2. Institutional Coordination Mechanisms

The Dubai Electronic Security Center (DESC) oversees the efforts of certification bodies to certify CSPs for government procurement.

Key Organizations

The **DDA** oversees policies and strategies to promote Dubai's digital transformation. The DDA is an umbrella organization that encompasses four entities respectively focused on data, security, statistics, and smart government. Each entity advances DDA's vision to promote a secure, data-centric government and city.

The **DESC** is an entity within the DDA that leads Dubai's efforts to ensure the cybersecurity of Dubai. In this capacity, DESC oversees the ISR and coordinates with Certification Bodies to certify technology vendors for government procurement through its *CSP Security Standard*.

Certification Bodies or third party certifiers are independent commercial entities accredited by DESC to assess and certify CSPs seeking government contracts against the *CSP Security Standard*. CSPs can select certification bodies through a public call process. In turn, these bodies do a light touch verification, a process of up to two days in which the Certification Body conducts an on-premises audit to confirm a CSP's compliance with the *CSP Security Standard*. The Certification Bodies themselves must have the ISO/IEC 17021-1:2015 certification to be a qualified certifier for DESC. So far, Dubai has approved one company as a Certification Body.

Procuring agencies are Dubai government and semi-government entities responsible for procuring cloud services that meet their requirements, based upon their data classification levels and other security and business needs.

Coordination Among Organizations

Government Agencies. The DDA and its entities work to educate and train officials within procuring agencies on how to understand their data and secure their ICT systems.

- DDE trains agency-level officials to be upskilled as data champions who understand and classify the data within their agencies.

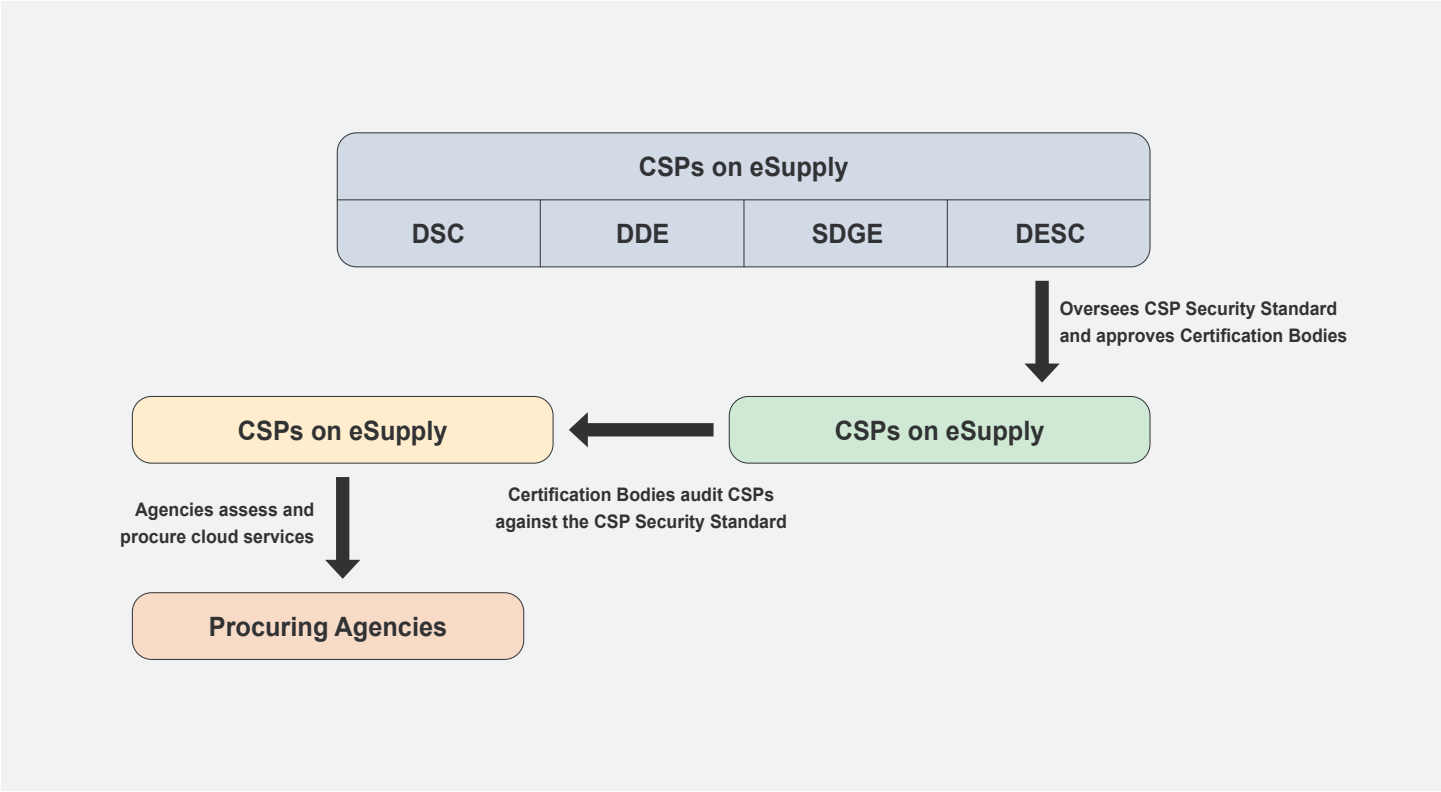
- DESC helps to establish ISO positions to oversee security aspects of their data environments. For larger institutions, the ISO unit is scaled to match the size of its operations, based on entity requirements. Each procuring agency should have at least one ISO position reporting directly to the head of the agency. This is to ensure independence of information security functions from IT, as per international best practices. Each procuring agency also has an Information Security Committee.

Government and Certification Bodies. DESC is responsible for approving Certification Bodies, which, in turn, audit the CSPs on DESC’s behalf. The CSPs themselves procure audit services from the Certification Bodies. The DESC is not directly involved with these audit activities.

Government and CSPs. The procuring agencies are ultimately responsible for assessing and purchasing cloud services from CSPs that are certified by Certification Bodies.

- ISR Officers collaborate with data champions, the Information Security Committee, Head of Agency, and others to make a risk-informed decision to procure cloud service.
- DESC aims to enable and empower procuring agencies to have the capacity to conduct these risk-based procurements without the need for major oversight.

> > >
FIGURE A5.1 - Notional Framework of the Dubai’s Institutional Mechanisms for Secure Cloud Procurements



Source: World Bank.

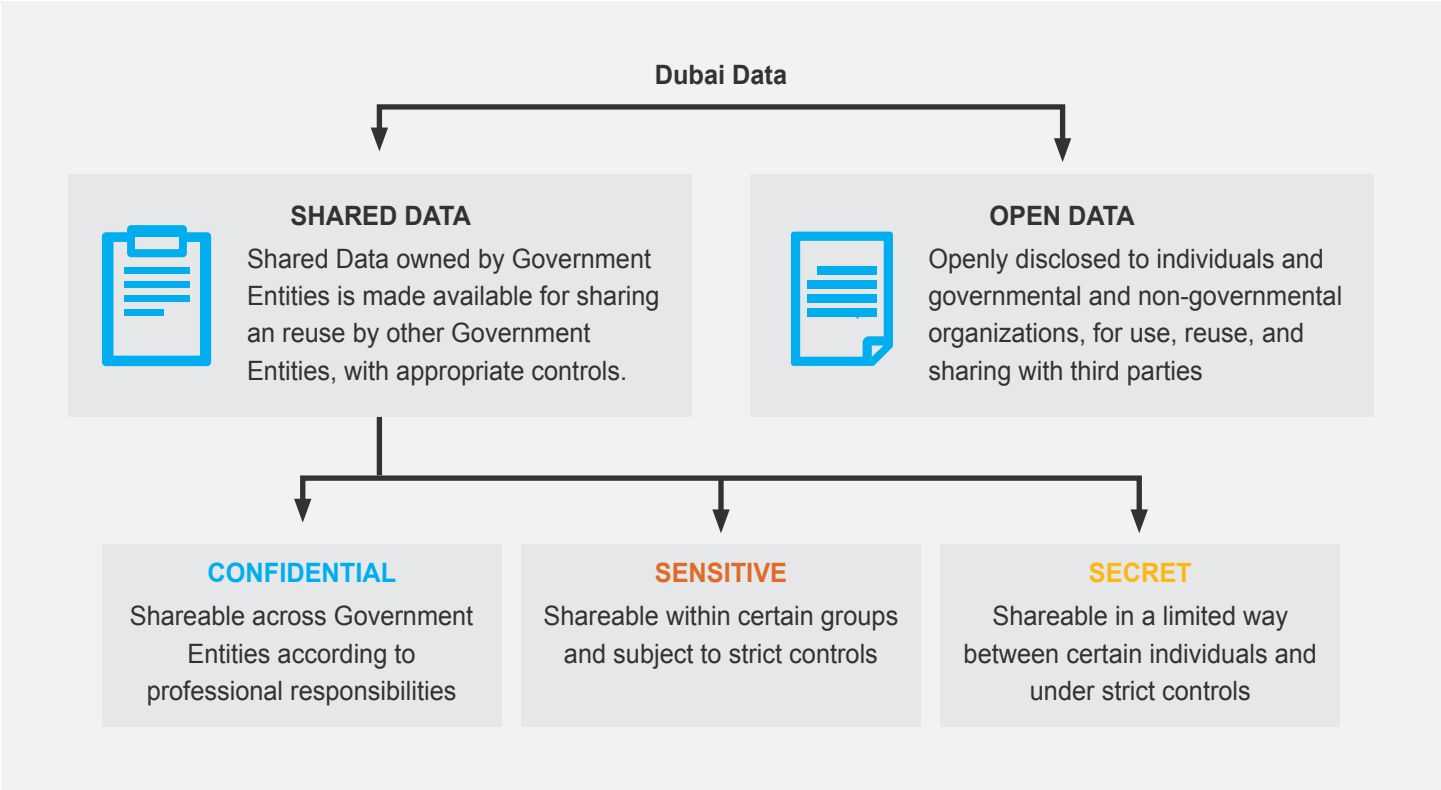
3. Data Classification and Security Framework

Dubai has established the Dubai Data Law, a data classification scheme and related cybersecurity and data privacy framework that supports its *CSP Security Standard*. Under Dubai's system, the DESC facilitates the certification of a CSP.

Data Classification

The DDE established the *Dubai Data Classification Framework* to enable government entities to classify their data as either Open or Shared. In turn, the DDE reviews and approves those classification decisions. The relationships between the different data classification categories are illustrated in Figure A5.2 below:

> > >
FIGURE A5.2 - Categories of Dubai Data



Source: Dubai Data Manual, <https://www.digitaldubai.ae/data/regulations>.

Under this framework, the four levels of data classification are defined as:

- **OPEN:** Data provided by the Dubai government or private sector entities to individuals, to be used or exchanged with third parties freely or subject to a limit.
- **SHARED-CONFIDENTIAL:** Data that, if shared through unrestricted disclosure or exchange, may cause limited damage to government bodies, companies, or individuals.

- **SHARED-SENSITIVE:** Data that, if shared through unrestricted disclosure or exchange, may cause significant damage to government bodies, companies, or individuals.
- **SHARED-SECRET:** Data that, if shared through unrestricted disclosure or exchange, may cause significant damage to the supreme interests of the country and very high damage to government bodies, companies, or individuals

CSPs hosting Open Data do not require security certifications. Those datasets



Data Residency

The DESC's *CSP Security Standard* requires CSPs must abide by *ISR:2017 13.2.1.1.1*, which forbids CSPs from handling Shared data for government entities outside the legal jurisdiction or geographical boundaries of the UAE. Dubai also requests that CSPs handling Shared data for government entities have a minimum of two data centers within the country's geographic jurisdiction to ensure resilience of their services in order to provide cloud services.¹²⁷ There is an exemption process for procuring agencies seeking to host shared data outside UAE, based on risk assessment.

Moreover, if a procuring agency handles data relevant to the security of Dubai, it is encouraged to consult with DESC before seeking public cloud solutions. Indeed, in these cases, it may be more appropriate for the procuring agency to use the DubaiPulse government cloud, which can host sensitive data.

Security Controls

The *CSP Security Standard* sets out security requirements for CSPs and procuring agencies using cloud services. Compliance with this standard is mandatory for all CSPs wishing to offer cloud services for procuring agencies.

The *CSP Security Standard* is based on the following international and national standards:

- ISO/IEC 27001:2013.
- ISO/IEC 27002:2013.

- ISO/IEC 27017:2015.
- CSA Cloud Controls Matrix 3.0.1 (Level 2 STAR).
- ISR V2.0 (also called ISR:2017).

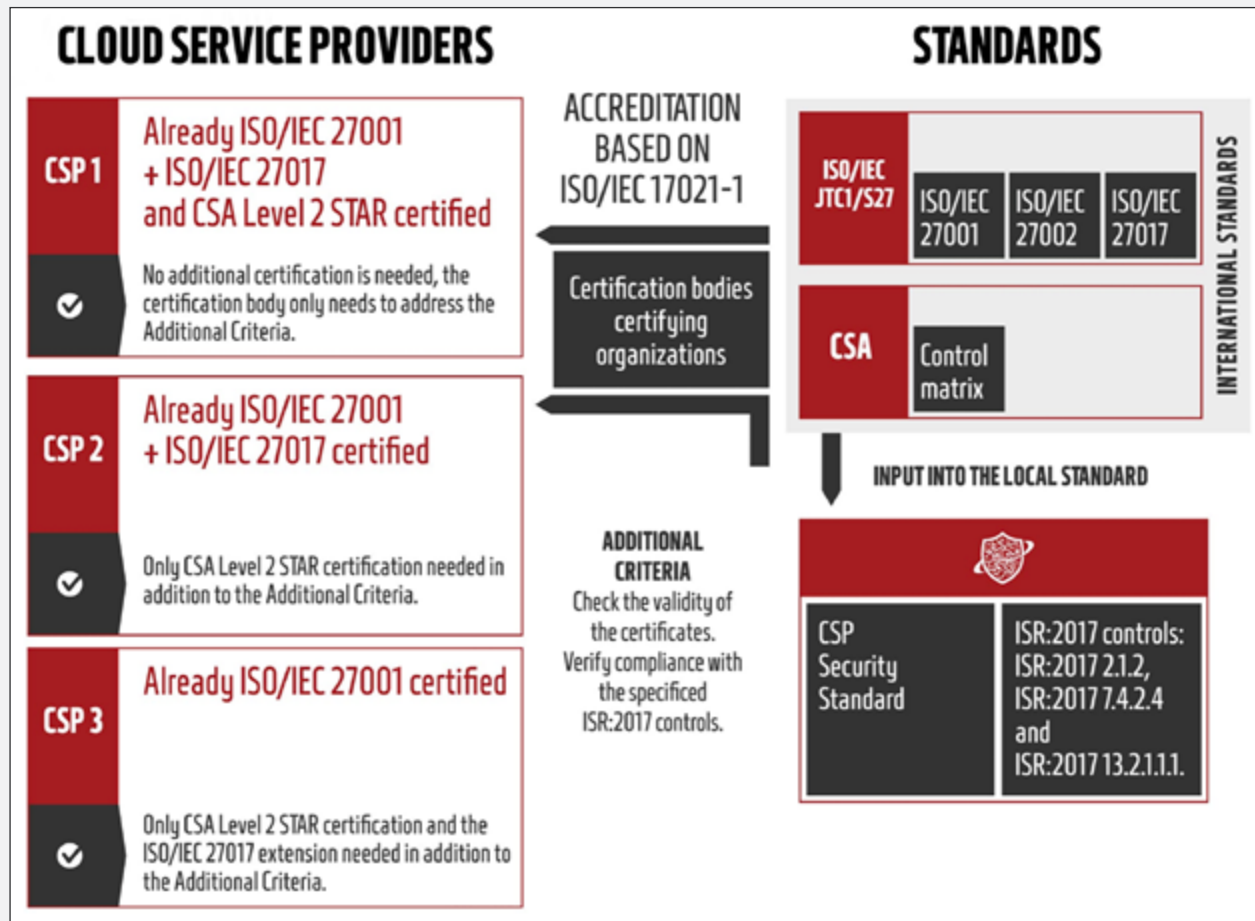
Preapproval Process

There are three key steps in the *CSP Security Standard* certification process:

- First, a CSP wishing to claim conformance to the *CSP Security Standard* must obtain an ISO/IEC 27001 certification with the ISO/IEC 27017 extension and the CSA Level 2 STAR certification.
- Second, the Certification Body must verify the validity of the CSP's ISO/IEC and CSA certificates. This audit can take as little as a half-day.
- Third, the Certification Body must verify the CSP's compliance with three selective ISR V2.0 controls:
 - ISR V2.0 2.1.2 (related to information asset management).
 - ISR V2.0 7.4.2.4 (related to media library and resource protection).
 - ISR V2.13.2.1.1.1 (related to restricting handling of classified data outside the UAE).

See Figure A5.3 below for a visual depiction of the certification process.

FIGURE A5.3 - CSP Security Standard Certification Process



Source: <https://www.desc.gov.ae/regulations/certifications/>.

If a CSP uses third-party co-located data centers, the certification process must ensure that this arrangement is sufficiently secure. Possibilities for such audit checks are:

- Inclusion of the data center(s) in the scope of existing or new ISO/IEC or CSA certificates.
- Assessment of the third-party controls, including risks related to third parties, that are applied by the CSP to ensure that adequate security is in place.

The DESC's certification process also allows SaaS and PaaS providers to inherit security controls of certified

IaaS. The basic principle is that every layer of the cloud stack should be certified, and if a layer is already certified, that layer does not need to be recertified. For example, if a SaaS provider contracts a certified hyperscaler such as Azure that has IaaS, it will only need to ensure certification of its SaaS offering, with the evidence that the underlying layer is certified.¹²⁸ In terms of continuous monitoring, CSPs certified under the *CSP Security Standard* are subject to annual on-site surveillance audits, where possible, and a recertification audit that takes place every three years.

4. Procurement Arrangements

Each government entity must assess a CSP's cloud services against its own security needs during the procurement phase.

Procuring agencies can purchase the cloud services of certified CSPs to handle any Shared data. For Open data, on the other hand, procuring agencies may choose any cloud service regardless of a CSP's certification status with no geographic limitations.

Procuring agencies handling Shared data must abide by ISR when procuring cloud services. Indeed, the ISR is intended to give procuring agencies the tools and guidelines to make risk-based decisions when purchasing cloud services. Each agency is expected to leverage its ISR Officer(s), Information Security Committee, and data champions to help make a risk-informed decision when procuring a public cloud service.

Each procuring agency is ultimately responsible for how it purchases a cloud service from a commercial provider. The Dubai Government's main online portal, eSupply, enables suppliers including CSPs to participate in online tenders or RFQs published by over 40 Dubai procuring agencies.¹²⁹ Any

company may simply register as a supplier on eSupply—there is no procurement process for being added to this portal. Procuring agencies may issue RFQs seeking cloud services from suppliers on eSupply, and can invite certain CSPs to issue a proposal/quotation in response to the RFQ.

Under eSupply, the specific procurement requirements for a cloud service varies depending on characteristics of each project. For example, procuring agencies may include various requirements, such as certification under the *CSP Security Standard*, as part of the RFQ process. Payment methods are also determined on a case-by-case basis by each procuring agency.

In future, Dubai aims to empower procuring agencies to use privacy-enhancing tools within their procured cloud services. For example, the “bring your own key/encryption” tool is a plug-in that would allow procuring agencies to provide their own cryptographic key to a CSP, which can in turn be integrated into its cloud solution. Dubai is currently analyzing this technology and the impact it might bring to secure data on the cloud.¹³⁰



Notes

1. For example, cloud solutions offer potential for increased energy efficiency of IT systems to help promote more environmentally sustainable IT ecosystems. See “Greening GovTech, Embracing a Green Digital Transition, Policy Note,” 2022. World Bank (Chapter 2.2.3.2.2).
2. These case studies differ from the United States’ FedRAMP model, which uses a tiered system to certify cloud services under the Low, Moderate, or High levels based upon security controls developed by NIST. “FedRAMP,” US Government. <https://www.fedramp.gov/>.
3. Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145, September 2011. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.
4. “Cloud Basics,” General Services Administration. <https://cic.gsa.gov/basics/cloud-basics>.
5. Cloud Basics.
6. Cloud Basics.
7. Vendor lock-in refers to a situation wherein a customer becomes dependent on a product or service regardless of quality, making it difficult to switch vendors.
8. Peter Mell and Timothy Grance, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145, 2011. <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf>.
9. Peter Mell and Timothy Grance.
10. Peter Mell and Timothy Grance.
11. Peter Mell and Timothy Grance.
12. World Bank, 2022, Government Migration to Cloud Ecosystems : Multiple Options, Significant Benefits, Manageable Risks, <https://openknowledge.worldbank.org/handle/10986/37556>.
13. “Certification,” ISO. <https://www.iso.org/certification.html>.

14. “Accreditation vs. Certification in Conformity Assessment,” ANSI National Accreditation Board. <https://anab.ansi.org/accreditationvscertificationinconformityassessment>.
15. “Certification,” ISO.
16. “Conformity Assessment,” NIST. <https://www.nist.gov/conformity-assessment>.
17. This Index rates countries based upon key aspects of four World Bank GovTech focus areas – enhancing service delivery, supporting core government systems, mainstreaming citizen engagement, and GovTech enablers – with a score of 1 being the highest maturity and 0 being the lowest maturity.
18. This Index rates countries based upon three dimensions of e-government (online services, telecommunications infrastructure, and human capital), with a score of 1 being the highest e-governance performance and 0 being the lowest e-governance performance.
19. This Index rates countries based upon capacity to promote a cloud-centric digital economy, with a score of 10 being the highest capacity and 0 being the lowest capacity.
20. “Australian Government Cloud Computing Policy (Version 3.0),” Australian Government (Department of Finance), October 2014. <https://www.ospi.es/export/sites/ospi/documents/documentos/Australian-Government-cloud-computing-policy.pdf>.
21. “Secure Cloud Strategy (Version 3),” DTA, October 2021. <https://www.dta.gov.au/sites/default/files/2021-10/DTA%20Secure%20Cloud%20Strategy%20-%20October%202021%20v3%20%28update%29.pdf>.
22. “ISMAP Came into Operation,” MIC, June 3, 2020. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/6/03_6.html.
23. “Government Cloud First policy,” CDDO, February 3, 2017. <https://www.gov.uk/guidance/government-cloud-first-policy>.
24. “About Digital Dubai,” Digital Dubai. <https://www.digitaldubai.ae/about-us>.
25. “Public Service Cloud Computing Determination and Directive,” DPSA, February 2, 2022. https://www.michalsons.com/wp-content/uploads/2022/04/egovernment_02_02_2022.pdf.
26. “National Data and Cloud Policy (Draft),” DCDT, April 1, 2021. https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf.
27. “Management Standards,” ISMAP. https://www.ismap.go.jp/csm/ja?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=277195e71b985910f18c65fa234bcbb8&spa=1.
28. “[Information Security Manual](#),” ACSC.
29. “[Cloud Security Controls Matrix](#),” ACSC.
30. “Cloud security guidance,” NCSC. <https://www.ncsc.gov.uk/collection/cloud>.

31. Azure provides an example of Total Cost of Ownership Calculator: <https://azure.microsoft.com/en-us/pricing/tco/calculator/>. Another Total Cost of Ownership Calculator example from AWS is provided: <https://calculator.aws/#/>.
32. Managing technical lock-in in the cloud – GOV.UK, www.gov.uk.
33. “Cloud Procurement: Best Practices for Public Sector Customers,” AWS, January 2017. <https://docplayer.net/100520847-Cloud-procurement-best-practices-for-public-sector-customers.html>.
34. PII is defined as any piece of information that confirms an individual’s identity. A person’s PII can include their Address; National Insurance Number or Social Security Number; Driver’s license; Financial information, including bank accounts; and Medical records. See: <https://www.isms.online/iso-27002/control-5-34-privacy-and-protection-of-pii/>.
35. Personal data classification and protection aligns with Chapter 6 of the World Development Report 2021 (WDR21), “Data policies, laws, and regulations: Creating a trust environment.”
36. The sharing and processing of public data can help to increase economic value. This policy effort aligns with the WDR21’s overall message that data produces economic value when processed and shared.
37. Source: Microsoft. 2021. “Best Practices for a Competitive Data Ecosystem” (internal document shared with authors).
38. Source: A Roadmap from Cross-Border Data Flows: Future Proofing Readiness and Cooperation in the New Data Economy, World Economic Forum, June 2020 white paper. https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.
39. The government approved the amendments to the Law on Management of State Information Resources; Ministry of the Economy and Innovation of the Republic of Lithuania (Irv.lt), March 23, 2022.
40. See “CLOUD Act Resources,” US Department of Justice. <https://www.justice.gov/dag/cloudact>.
41. “ISMAP Came into Operation,” MIC, June 3, 2020. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/6/03_6.html.
42. ISMAP Came into Operation.
43. “Study Group on Security Assessment of Cloud Services Compiles its Discussion Results into Report,” METI, January 30, 2020. https://www.meti.go.jp/english/press/2020/0130_002.html.
44. Study Group on Security Assessment of Cloud Services.
45. “ISMAP Overview,” ISMAP. https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010301.
46. National Center of Incident Readiness and Strategy for Cybersecurity (NISC). <https://www.nisc.go.jp/eng/index.html>.

47. "Assessors List," ISMAP. https://www.ismap.go.jp/csm?id=audit_institution_list.
48. Interview with IPA on July 20, 2022.
49. "Cloud Service List," ISMAP. https://www.ismap.go.jp/csm?id=cloud_service_list.
50. "ISMAP Overview," ISMAP. https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010301.
51. "Standards for Security Categorization of Federal Information and Information Systems, FIPS 199," NIST, February 2004. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf>.
52. "ISMAP Overview," ISMAP. https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010301.
53. "Management Standards," ISMAP. https://www.ismap.go.jp/csm/ja?id=kb_article_view&sysparm_article=KB0010028.
54. "ISMAP Overview," ISMAP. https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010301.
55. "Australian Government Cloud Computing Policy (Version 3.0)," *Australian Government (Department of Finance)*, October 2014. <https://www.ospi.es/export/sites/ospi/documents/documentos/Australian-Government-cloud-computing-policy.pdf>.
56. Justin Hendry, "DTA pushes Commonwealth to adopt more cloud," IT News, February 1, 2018. <https://www.itnews.com.au/news/dta-pushes-commonwealth-to-adopt-more-cloud-484234>.
57. Justin Hendry, "DTA pushes Commonwealth to adopt more cloud."
58. "Secure Cloud Strategy (Version 3)," DTA, October 2021. <https://www.dta.gov.au/sites/default/files/2021-10/DTA%20Secure%20Cloud%20Strategy%20-%20October%202021%20v3%20%28update%29.pdf>.
59. "Anatomy of a Cloud Assessment and Authorisation," ACSC. <https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation>.
60. "[The Cloud Security Assessment Report Template](#)," ACSC.
61. "[Information Security Manual](#)," ACSC.
62. "[Cloud Security Controls Matrix](#)," ACSC.
63. "Protective Security Policy Framework," *Attorney-General's Department, Australia*. <https://www.protectivesecurity.gov.au/>.
64. "Cloud Computing Security Considerations," ACSC. <https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>.
65. "Digital Transformation Agency." <https://www.dta.gov.au/>.
66. "Australian Signals Directorate." <https://www.asd.gov.au/>.

67. "Australian Cyber Security Operations Centre." <https://www.cyber.gov.au/>.
68. "Who are IRAP Assessors?" ACSC. <https://www.cyber.gov.au/acsc/view-all-content/programs/irap/who-are-irap-assessors>.
69. "IRAP Assessors," ACSC. <https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors>.
70. "Cloud Marketplace," BuyICT, DTA. https://www.buyict.gov.au/sp?id=marketplace_landing&marketplace=20d4561edb261c106529773c349619b7&kb=KB0010616&path=buying.
71. "Cloud Marketplace," BuyICT, DTA.
72. "Cloud Marketplace."
73. "Hosting Certification Framework," DTA. <https://www.dta.gov.au/our-projects/hosting-strategy/hosting-certification-framework>.
74. "Framework Overview," DTA. <https://www.hostingcertification.gov.au/framework>.
75. "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, SP 800-37 Rev. 2, NIST, December 2018. <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>.
76. "Cyber Security Principles," ACSC. <https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-principles>.
77. "[Cloud Security Controls Matrix](#)," ACSC.
78. "Anatomy of a Cloud Assessment and Authorisation," ACSC. <https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation>.
79. "IRAP resources," ACSC. <https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-resources>.
80. "Cloud Marketplace," DTA. https://www.buyict.gov.au/sp?id=marketplace_landing&marketplace=20d4561edb261c106529773c349619b7&path=buying&kb=KB0010616.
81. [Cloud Sourcing Contract Template](#); [Cloud Services Minimum Terms](#).
82. "Government Cloud First policy," CDDO, February 3, 2017, <https://www.gov.uk/guidance/government-cloud-first-policy>.
83. "Government Cloud First policy," CDDO.
84. "Digital Marketplace," CCS. <https://www.digitalmarketplace.service.gov.uk/>.
85. "Ultimate Guide to G-Cloud," AdviceCloud. <https://advice-cloud.co.uk/ultimate-guide-gcloud/>.
86. "Cloud Compute," CCS. <https://www.crowncommercial.gov.uk/agreements/RM6111>.
87. "Cloud security guidance," NCSC. <https://www.ncsc.gov.uk/collection/cloud>.

88. "Security policy framework," UK Government, February 8, 2022, <https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>.
89. "Minimum Cyber Security Standard," UK Government, June 25, 2018, <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>.
90. "Risk management guidance," NCSC. <https://www.ncsc.gov.uk/collection/risk-management-collection>.
91. "Security," GOV.UK Platform as a Service. <https://www.cloud.service.gov.uk/security/>.
92. <https://www.ncsc.gov.uk/blog-post/announcing-iasme-consortium-as-our-new-cyber-essentials-partner>.
93. "About Cyber Essentials," NCSC. <https://www.ncsc.gov.uk/cyberessentials/overview>.
94. "Introducing the Government Security Classifications Core briefing for 3rd Party Suppliers," UK Cabinet Office, October 2013. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf.
95. "Cloud guide for the public sector," CDDO, February 8, 2021. <https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector>.
96. "Digital Marketplace Frameworks: G-13 Cloud Declarations," Github. [digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/declaration_at_main · Crown-Commercial-Service/digitalmarketplace-frameworks · GitHub](https://github.com/digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/declaration_at_main_Crown-Commercial-Service/digitalmarketplace-frameworks); "Digital Marketplace Frameworks: G-13 Cloud Services," Github. [digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/services_at_main · Crown-Commercial-Service/digitalmarketplace-frameworks · GitHub](https://github.com/digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/services_at_main_Crown-Commercial-Service/digitalmarketplace-frameworks).
97. "Securing your information," UK Government, May 21, 2018. <https://www.gov.uk/service-manual/technology/securing-your-information>.
98. However, the UK government notes that "if your service handles information that's classified as 'secret' or 'top secret,' then you should ask for specialist advice from your department or agency security team."
99. "Securing your cloud environment for services," UK Government. <https://www.gov.uk/service-manual/technology/securing-your-cloud-environment>.
100. "Security policy framework," UK Government, February 8, 2022. <https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>.
101. "Risk management guidance," NCSC. <https://www.ncsc.gov.uk/collection/risk-management-collection>.
102. "Secure development and deployment guidance," NCSC. <https://www.ncsc.gov.uk/collection/developers-collection>.
103. "G-Cloud 12 Framework Agreement," CCS. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/927650/G-Cloud-12-Framework-Agreement.pdf.

104. “Digital Marketplace Frameworks: G-13 Cloud Declarations,” Github. [digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/declaration_at_main · Crown-Commercial-Service/digitalmarketplace-frameworks · GitHub](https://github.com/digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/declaration_at_main_Crown-Commercial-Service/digitalmarketplace-frameworks); “Digital Marketplace Frameworks: G-13 Cloud Services,” Github. [digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/services_at_main · Crown-Commercial-Service/digitalmarketplace-frameworks · GitHub](https://github.com/digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/services_at_main_Crown-Commercial-Service/digitalmarketplace-frameworks).
105. “Introduction to cloud security,” NCSC. <https://www.ncsc.gov.uk/collection/cloud/introduction-to-cloud-security>.
106. [RM6111-Framework-Terms-v3.3.docx \(live.com\)](https://live.com/RM6111-Framework-Terms-v3.3.docx).
107. “G-Cloud 12 Call-Off Contract,” CCS. <https://assets.crowncommercial.gov.uk/wp-content/uploads/G-Cloud-12-Call-Off-Contract-v16-PDF.pdf>.
108. “Ultimate Guide to G-Cloud,” AdviceCloud. <https://advice-cloud.co.uk/ultimate-guide-gcloud/>.
109. “Managing technical lock-in in the cloud,” CDDO, December 17, 2019. <https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud>.
110. “National e-government strategy and roadmap,” DTPS. November 10, 2017. https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf.
111. “National Data and Cloud Policy (Draft)”, DCDT, April 1, 2021. https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf.
112. “Public Service Cloud Computing Determination and Directive,” DPSA, February 2, 2022. https://www.michalsons.com/wp-content/uploads/2022/04/egovernment_02_02_2022.pdf.
113. “Minimum Information Security Standards,” South African Government, December 4, 1996. [https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20\(MISS\).pdf](https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf)
114. “Directive on Public Service Information Security,” DPSA, 2022. https://www.dpsa.gov.za/dpsa2g/documents/ogcio/2022/egov_21_06_2022_directive.pdf.
115. Directive on Public Service Information Security, DPSA.
116. “Protection of Personal Information Act,” South African Government, November 26, 2013. https://www.dffe.gov.za/sites/default/files/legislations/popia04of2013_vol581no37067.pdf.
117. “Promotion of Access to Information Act of 2000,” South African Government, February 2, 2000. [http://juta/nxt/print.asp?NXTScript=nxt/gateway.dll&NXTHost=jut\(dffe.gov.za\)](http://juta/nxt/print.asp?NXTScript=nxt/gateway.dll&NXTHost=jut(dffe.gov.za)).
118. “Electronic Communications and Transactions Act, 2002,” South African Government, August 2, 2002. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.
119. “Public Service Cloud Computing Determination and Directive,” DPSA, February 2, 2022. https://www.michalsons.com/wp-content/uploads/2022/04/egovernment_02_02_2022.pdf.

120. See pages 14-18 of “Public Service Cloud Computing Determination and Directive,” DPSA, February 2, 2022. https://www.michalsons.com/wp-content/uploads/2022/04/egovernment_02_02_2022.pdf.
121. “About Digital Dubai,” Digital Dubai. <https://www.digitaldubai.ae/about-us>.
122. “KPI Card (Percentage of Applications Hosted on Cloud),” Dubai Government Excellence Program.
123. “Certifications,” Dubai Electronic Security Center. <https://www.desc.gov.ae/regulations/certifications/>.
124. “Information Security Regulation Version 2.0,” Dubai Electronic Security Center, 2017.
125. “Standards and Policies,” Dubai Electronic Security Center. <https://www.desc.gov.ae/regulations/standards-policies/>.
126. “Dubai Pulse”, <https://www.dubaipulse.gov.ae/>.
127. Conversation with Bushra Al Blooshi, July 28, 2022.
128. Conversation with Bushra Al Blooshi, July 28, 2022.
129. “eSupply,” Government of Dubai. <https://esupply.dubai.gov.ae/esupply/web/index.html>.
130. Conversation with Bushra Al Blooshi, July 28, 2022.



References

AdviceCloud. “Ultimate Guide to G-Cloud.” <https://advice-cloud.co.uk/ultimate-guide-gcloud/>.

Amazon Web Services. 2017. Cloud Procurement: *Best Practices for Public Sector Customers*. January 2017. <https://docplayer.net/100520847-Cloud-procurement-best-practices-for-public-sector-customers.html>.

ANSI National Accreditation Board. 2022. “Accreditation vs. Certification in Conformity Assessment.” Webinar. September 29, 2022. <https://anab.ansi.org/accreditationvscertificationinconformityassessment>.

Australian Attorney-General’s Department. “Protective Security Policy Framework.” <https://www.protectivesecurity.gov.au/>.

Australian Cyber Security Centre. 2021. “Anatomy of a Cloud Assessment and Authorisation.” October 2021. <https://www.cyber.gov.au/acsc/view-all-content/publications/anatomy-cloud-assessment-and-authorisation>.

Australian Cyber Security Centre. 2021. “Cloud Computing Security Considerations.” October 2021. <https://www.cyber.gov.au/acsc/view-all-content/publications/cloud-computing-security-considerations>.

Australian Cyber Security Centre. 2022. “Cloud Security Controls Matrix.” December 1, 2022. <https://www.cyber.gov.au/sites/default/files/2022-12/Cloud%20Controls%20Matrix%20Template%20%28December%202022%29.xlsx>.

Australian Cyber Security Centre. 2022. “Cyber Security Principles.” June 16, 2022. <https://www.cyber.gov.au/acsc/view-all-content/advice/cyber-security-principles>.

Australian nCyber Security Centre. 2022. “Information Security Manual.” December 1, 2022. <https://www.cyber.gov.au/sites/default/files/2022-12/Information%20Security%20Manual%20%28December%202022%29.pdf>.

Australian Cyber Security Centre. 2022. “The Cloud Security Assessment Report Template.” July 2022. <https://www.cyber.gov.au/sites/default/files/2022-07/Cloud-Security-Assessment-Report-Template-06-July-2022.docx>.

Australian Cyber Security Centre. “Australian Cyber Security Operations Centre.” <https://www.cyber.gov.au/>.

Australian Cyber Security Centre. "IRAP Assessors." <https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-assessors>.

Australian Cyber Security Centre. "IRAP Resources." <https://www.cyber.gov.au/acsc/view-all-content/programs/irap/irap-resources>.

Australian Cyber Security Centre. "Who are IRAP Assessors?" <https://www.cyber.gov.au/acsc/view-all-content/programs/irap/who-are-irap-assessors>.

Australian Department of Finance. 2014. *Australian Government Cloud Computing Policy (Version 3.0)*. October 2014. <https://www.ospi.es/export/sites/ospi/documents/documentos/Australian-Government-cloud-computing-policy.pdf>.

Australian Department of Public Service and Administration. 2022. *Public Service Cloud Computing Determination and Directive*. February 2, 2022. https://www.michalsons.com/wp-content/uploads/2022/04/egovernment_02_02_2022.pdf.

Australian Digital Transformation Agency. 2021. *Secure Cloud Strategy (Version 3)*. <https://www.dta.gov.au/sites/default/files/2021-10/DTA%20Secure%20Cloud%20Strategy%20-%20October%202021%20v3%20%28update%29.pdf>.

Australian Digital Transformation Agency. "Cloud Marketplace." https://www.buyict.gov.au/sp?id=marketplace_landing&marketplace=20d4561edb261c106529773c349619b7&kb=KB0010616&path=buying.

Australian Digital Transformation Agency. "Digital sourcing contract templates". December 2020. https://www.buyict.gov.au/sp?id=resources_and_policies&kb=KB0010684&kbparent=KB0010686 (note: link under the subheading "Cloud Services Minimum Terms Template").

Australian Digital Transformation Agency. "Digital sourcing contract templates". December 2020. https://www.buyict.gov.au/sp?id=resources_and_policies&kb=KB0010684&kbparent=KB0010686 (note: link under the subheading "Cloud Sourcing Contract Template").

Australian Digital Transformation Agency. "Digital Transformation Agency." <https://www.dta.gov.au/>.

Australian Digital Transformation Agency. "Framework Overview." <https://www.hostingcertification.gov.au/framework>.

Australian Digital Transformation Agency. "Hosting Certification Framework." <https://www.dta.gov.au/our-projects/hosting-strategy/hosting-certification-framework>.

Australian Signals Directorate. "Australian Signals Directorate." <https://www.asd.gov.au/>.

Digital Dubai. "About Digital Dubai." <https://www.digitaldubai.ae/about-us>.

Digital Dubai. "Regulations." <https://www.digitaldubai.ae/data/regulations>.

Dubai Electronic Security Center. 2017. *Information Security Regulation (Version 2.0)*.

Dubai Electronic Security Center. "Certifications." <https://www.desc.gov.ae/regulations/certifications/>.

Dubai Electronic Security Center. “Standards and Policies.” <https://www.desc.gov.ae/regulations/standards-policies/>.

Dubai Smart Government. “Dubai Pulse.” <https://www.dubaipulse.gov.ae/>.

Dubai Smart Government. “eSupply.” <https://esupply.dubai.gov.ae/esupply/web/index.html>.

Hendry, Justin. 2018. “DTA pushes Commonwealth to adopt more cloud.” IT News. February 1, 2018. <https://www.itnews.com.au/news/dta-pushes-commonwealth-to-adopt-more-cloud-484234>.

International Standards Organization. “Certification.” <https://www.iso.org/certification.html>.

Japan Information System Security Management and Assessment Program. “Assessors List.” https://www.ismap.go.jp/csm?id=audit_institution_list.

Japan Information System Security Management and Assessment Program. “Cloud Service List.” https://www.ismap.go.jp/csm?id=cloud_service_list.

Japan Information System Security Management and Assessment Program. “Management Standards.” https://www.ismap.go.jp/csm/ja?id=kb_article_view&sysparm_article=KB0010028&sys_kb_id=277195e71b985910f18c65fa234bcbb8&spa=1.

Japan Ministry of Economy, Trade, and Industry. 2020. “Study Group on Security Assessment of Cloud Services Compiles its Discussion Results into Report.” January 30, 2020. https://www.meti.go.jp/english/press/2020/0130_002.html.

Japan Ministry of Internal Affairs and Communications. 2020. “ISMAP Came into Operation.” June 3, 2020. https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2020/6/03_6.html.

Japan National Center of Incident Readiness and Strategy for Cybersecurity. “National Center of Incident Readiness and Strategy for Cybersecurity.” <https://www.nisc.go.jp/eng/index.html>.

Mell, Peter and Grance, Timothy. 2011. *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-145)*. September 2011. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>.

Microsoft. 2021. “Best Practices for a Competitive Data Ecosystem” (internal document shared with authors).

Microsoft. 2022. “Defending Ukraine: Early Lessons from the Cyber War.” June 22, 2022. <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.

Microsoft. 2022. “Extending our vital technology support for Ukraine.” November 3, 2022. <https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/>.

Microsoft. 2022. “Special Report: Ukraine - An overview of Russia’s cyberattack activity in Ukraine.” April 27, 2022. <https://www.iisf.ie/Microsoft-Special-report-Ukraine-Russia-Cyberattack-activity>.

Oracle and KPMG. 2020. *Demystifying the Cloud Shared Responsibility Security (Volume 2)*. <https://www.oracle.com/a/ocom/docs/cloud/oracle-ctr-2020-shared-responsibility.pdf>.

South African Department of Communications and Digital Technologies. 2021. "National Data and Cloud Policy (Draft)." April 1, 2021. https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf.

South African Department of Public Service and Administration. 2022. *Directive on Public Service Information Security*. June 7, 2022. https://www.dpsa.gov.za/dpsa2g/documents/ogcio/2022/egov_21_06_2022_directive.pdf.

South African Department of Telecommunications and Postal Services. 2017. *National e-government strategy and roadmap*. November 7, 2017. https://www.gov.za/sites/default/files/gcis_document/201711/41241gen886.pdf.

South African Government. 1996. *Minimum Information Security Standards*. December 6, 1996. [https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20\(MISS\).pdf](https://www.sita.co.za/sites/default/files/documents/MISS/Minimum%20Information%20Security%20Standards%20(MISS).pdf).

South African Government. 2002. *Electronic Communications and Transactions Act, 2002*. August 2, 2002. https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf.

South African Government. 2013. *Protection of Personal Information Act*. November 26, 2013. https://www.dffe.gov.za/sites/default/files/legislations/popia04of2013_vol581no37067.pdf.

South African Revenue Service. 2000. "Promotion of Access to Information Act of 2000." October 15, 2021. <https://www.sars.gov.za/legal-counsel/primary-legislation/promotion-of-access-to-information-act-2000-paia/>.

TurningCloud Solutions. 2021. "4 Cloud Deployment Models: Their advantages and disadvantages." June 21, 2021. <https://www.turningcloud.com/blog/cloud-deployment-models/>.

UK Cabinet Office. 2013. *Introducing the Government Security Classifications Core briefing for 3rd Party Suppliers*. October 2013. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251481/Government-Security-Classifications-Supplier-Briefing-Oct-2013.pdf.

UK Cabinet Office. 2018. "Government Security Classifications." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018-Government-Security-Classifications-2.pdf.

UK Cabinet Office. 2018. "Minimum Cyber Security Standard." June 25, 2018. <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>.

UK Cabinet Office. 2022. "Security policy framework." December 2, 2022. <https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework>.

UK Central Digital and Data Office. 2019. "Managing technical lock-in in the cloud." December 17, 2019. <https://www.gov.uk/guidance/managing-technical-lock-in-in-the-cloud>.

UK Central Digital and Data Office. 2021. "Cloud guide for the public sector." February 8, 2021. <https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector>.

UK Central Digital and Data Office. 2022. "Government Cloud First policy." July 21, 2022. <https://www.gov.uk/guidance/government-cloud-first-policy>.

UK Crown Commercial Services. "Cloud Compute." <https://www.crowncommercial.gov.uk/agreements/RM6111>.

UK Crown Commercial Services. "Digital Marketplace." <https://www.digitalmarketplace.service.gov.uk/>.

UK Crown Commercial Services. "Digital Marketplace Frameworks: G-13 Cloud Declarations." digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/declaration_at_main · Crown-Commercial-Service/digitalmarketplace-frameworks · GitHub.

UK Crown Commercial Services. "Digital Marketplace Frameworks: G-13 Cloud Services." digitalmarketplace-frameworks/frameworks/g-cloud-13/questions/services_at_main · Crown-Commercial-Service/digitalmarketplace-frameworks · GitHub.

UK Crown Commercial Services. *G-Cloud 12 Call-Off Contract (RM1557.12)*. 2022. <https://assets.crowncommercial.gov.uk/wp-content/uploads/G-Cloud-12-Call-Off-Contract-v16-PDF.pdf>.

UK Crown Commercial Services. *G-Cloud 12 Framework Agreement (RM1557.12)*. 2022. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/927650/G-Cloud-12-Framework-Agreement.pdf.

UK Government. 2018. "Securing your information." May 21, 2018. <https://www.gov.uk/service-manual/technology/securing-your-information>.

UK Government Platform-As-A-Service. "Security." <https://www.cloud.service.gov.uk/security/>.

UK National Cyber Security Centre. 2018. "Risk management guidance." November 16, 2018. <https://www.ncsc.gov.uk/collection/risk-management-collection>.

UK National Cyber Security Centre. 2018. "Secure development and deployment guidance." November 22, 2018. <https://www.ncsc.gov.uk/collection/developers-collection>.

UK National Cyber Security Centre. 2019. "Announcing IASME Consortium as our new Cyber Essentials Partner." October 7, 2019. <https://www.ncsc.gov.uk/blog-post/announcing-iasme-consortium-as-our-new-cyber-essentials-partner>.

UK National Cyber Security Centre. 2021. "Securing your cloud environment for services." February 15, 2021. <https://www.gov.uk/service-manual/technology/securing-your-cloud-environment>.

UK National Cyber Security Centre. 2022. "Cloud security guidance." May 10, 2022. <https://www.ncsc.gov.uk/collection/cloud>.

UK National Cyber Security Centre. 2022. "Introduction to cloud security." May 10, 2022. <https://www.ncsc.gov.uk/collection/cloud/introduction-to-cloud-security>.

UK National Cyber Security Centre. “About Cyber Essentials.” <https://www.ncsc.gov.uk/cyberessentials/overview>.

US Department of Justice. 2022. “CLOUD Act Resources.” November 29, 2022. <https://www.justice.gov/criminal-oia/cloud-act-resources>.

US Federal Risk and Authorization Management Program. “Securing Cloud Services.” <https://www.fedramp.gov/>.

US General Services Administration. “Cloud Basics.” <https://cic.gsa.gov/basics/cloud-basics>.

US National Institute of Standards and Technology. 2004. *Standards for Security Categorization of Federal Information and Information Systems, FIPS 199*. February 2004. <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf>.

US National Institute of Standards and Technology. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (SP 800-37 Rev. 2)*. December 2018. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>.

US National Institute of Standards and Technology. “Conformity Assessment.” <https://www.nist.gov/conformity-assessment>.

World Bank. 2022. “Greening GovTech, Embracing a Green Digital Transition, Policy Note.” Note: Draft.

World Bank. 2022. *Government Migration to Cloud Ecosystems: Multiple Options, Significant Benefits, Manageable Risks*. Report. June 10, 2022. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099530106102227954/p17303207ce6cf0420bcd006737c2750450>.

World Economic Forum. 2020. *A Roadmap from Cross-Border Data Flows: Future Proofing Readiness and Cooperation in the New Data Economy*. June 2020. https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf.

Supported by the GovTech Global Partnership - www.worldbank.org/govtech

