DGX WORKGROUP ON CLOUD

August 2023

Prepared by: Government Technology Agency, Singapore

In collaboration with: Government of Australia, Israel, Finland, New Zealand and United Nations

Contents

Acknowledgements

This report has been developed under the DGX WorkGroup for Cloud, led by Richard Tay (Singapore, Senior Director for Government Infrastructure Group, Government Technology Agency), with members from Government of Australia, Israel, Finland, New Zealand and United Nations.

We would like to thank the following workgroup members for their valuable contributions and generous sharing which have greatly benefited the development of this report.

- [Singapore – Lead] Richard Tay, Senior Director Government Infrastructure Group, GovTech
- [Australia] Andrew Morrison, CTO, Australian Digital Transformation Agency
- [Israel] Karen Bar-Lev, CTO and Head of Cloud CoE, Israel Government
- [Finland] Jyri Vuorikallio, Senior Specialist, Ministry of Finance
- [Singapore] Chia Hsiao Ming, Director, Government Digital Services Central, GovTech
- [Singapore] Stanley Tsang, Distinguished Engineer and Senior Director (Special Projects), Cybersecurity Agency Singapore
- [New Zealand] Tony Eyles, Director Cloud Programme, Department of Internal Affairs
- [New Zealand] Sarah Dickson-Johansen, Principal Advisor, Planning, Performance and Systems, Department of Internal Affairs
- [New Zealand] Serena Chui, Principal Advisor, Digital Public Service, Digital Public Service, Department of Internal Affairs
- [United Nations] Kwok Wai Min, Senior Governance and Public Administration Officer, UN Department of Economic and Social Affairs (UN DESA)

Supported by:

- [Singapore] Karen Kee, Deputy Director, Technology Management Office, GovTech
- [Singapore] Koh Lay Hian, Senior Infrastructure Architect, Government Infrastructure Group, GovTech
- [Singapore] Low Rui Ru, Assistant Manager, Technology Management Office, GovTech

Executive Summary

With the rapid development in public cloud infrastructure, it is now a mainstream consideration for quick deployment of solutions and services to support the needs of both the public and government organisations. Taking into the considerations of data sovereignty and matters involving national interests, government organisations generally put in place various guidelines and guardrails in the approach towards cloud adoption.

The report aims to inform the audience about the **landscape and approach of cloud adoption in government**, in particular from DGX2023 cloud working group member countries – Australia, Finland, Israel, New Zealand, Singapore and United Nations. This report provides a **general view across government organisations in their journey for cloud adoption and discusses the considerations, measures and central services implemented** to facilitate their ministries and agencies to be able to roll out services with ease to serve citizens and businesses effectively.

All member countries adopted a '**Cloud First' approach** where it categorises and identifies systems suitable to be moved to cloud to reap its benefits:

i. Australia - Digital Sourcing Consider First Policy, Hosting Certification Framework, Technology and Cloud Security Guidance
ii. Finland - Cloud Service Guidelines and Project Cirrus
iii. Israel - Cloud First Policy, Cloud Journey methodology, Nimbus Project
iv. New Zealand - Cloud First Policy
v. Singapore - Commercial Cloud First Policy

With the various countries' collective experience assisting government organisations in their move to cloud, different measures were derived to address unique circumstances and make the transition smoother. **Knowledge management** is key with the setting up of **communities** and **sharing platforms**, delivering **playbooks, migration strategies** and **conducting of training extensively to the ecosystem**. Pushing along **IT policies and** procurement in alignment is also important in order to not impede the progress. Lastly, effective cost management in day 2 operations also needs to be adopted and refined with **FinOps**.

A further push could be done with the **offering of central services** for which cloud native services could not directly be adopted for the unique government use cases. An example shared by Israel in their offering of **Cloud Strategy Shared services** include the **Government Landing Zone, Data Highway, Internal Government Code Share, a common Identity Management service, Mail Platform and IT Service Management services** to be used to serve their ministry systems deployed in cloud. Australia launched the **Australian Government Architecture (AGA)** which provides transparency in the capability requirements needed to be built by agencies and industries. Singapore provides the **Singapore Government Tech Stack (SGTS)** with a vision to modernise development practice across agencies to help build secure systems in alignment with cloud platforms offered.

In the example of Singapore, there is also a focus on the **standardisation and offering of developer tools and platforms** for the cloud to accelerate the migration of applications to cloud. A centralised toolchain platform for example, allows development teams to leverage on reusable components, and to incorporate templates for security policies and compliance as part of automation. All these provide **better visibility and observability to drive DevSecOps practices** for government systems on the cloud.

Overview

1. The DGX Cloud Workgroup consists of members from Australia, Finland, Israel, New Zealand, United Nations and Singapore (lead). The report captures the Cloud adoption landscape across governments, including challenges, approaches, and learning points in Cloud best practices from member countries' experience in their cloud journey.

2. The workgroup agreed to focus on the following key discussion topics with the intent to share the learnings and approach to drive acceleration of cloud adoption.

    A. **Policies on Cloud Hosting**
    B. **Measures to further drive Cloud Adoption**
    C. **Centralised Services as an acceleration to Cloud**

A. Policies on Cloud Hosting

3. Cloud hosting policies serve as a general reference on the journey towards cloud adoption approach. The approach involves cloud adoption models, as well as considerations on sovereignty, jurisdiction risks, etc based on members' experience. The policies would also have to be refreshed periodically depending on the readiness and evolving technology readiness. The key areas addressed in this section would include:

    a. Cloud landscape and policies – this includes statistics and trending from member countries, including IaaS, PaaS and SaaS adoption
    b. Data classification framework – this includes perspective of how each countries' classification levels matches up in general, and the hosting approach for the corresponding classification levels

Cloud landscape and policies

4. Member countries are in various stages of cloud adoption and each has developed a strategy and put in place policies suitable for the particular stage of cloud adoption. In general, key guiding principles are in place to drive towards a 'cloud first' approach where it categorises and identifies systems suited to be moved to cloud to reap its benefits.

    Australia – Australia has various policy mechanisms to support cloud adoption, ranging from sourcing policy constructs to cybersecurity advice. Key mechanisms in place are as follows:

    a. The Digital Sourcing Consider First Policy (Resources and policies – BuyICT)
        - Came into effect from July 2019. The intent of the policy is to the apply to any investment in digital products/and or services with an expected or realised whole-of-life cost of $80,000AUD or greater.
        - A Principle within this policy is to Align with whole of Government Requirements, with Cloud First (Principle 5.3) requires agencies to consider cloud solutions and to follow the Secure Cloud strategy.

    b. The Hosting Certification Framework (Framework | Hosting Certification Framework)
        - The Hosting Certification Framework, delivered by the Department of Home Affairs, supports agencies to make a risk-based decision on the cloud services and systems

available and applies to anyone in the Australian Government needing hosting arrangements for sensitive government data, whole of government systems and systems rated at the classification level of PROTECTED.

- There are three levels of Certification – Strategic, Assured, and Uncertified:
  - Strategic as the highest level of certification and specifies increased security controls building on Assured.
  - Assured provides safeguards against change of ownership or control
  - Uncertified offers minimal protections to government and may be used for non-sensitive data.

c. Technology Guidance (Using cloud in government | Digital Transformation Agency (dta.gov.au))
   - Technology Guidance has been developed to support agencies in their transition to cloud through the Digital Transformation Agency's Help and Advice with 'Using Cloud in Government'.
   - General advice on how to establish funding for cloud, and the transition to operational expenditure over more traditional means of operational expense allocation.
   - Types of hosting approaches from Software as a Service (SaaS), Platform (PaaS), and Infrastructure (IaaS)

d. Cloud Security Guidance (Cloud security guidance | Cyber.gov.au)
   - The Australian CyberSecurity Centre has developed a process around assessment cloud security and important considerations for organisations using cloud vendors (or cloud service providers).
   - The advice has been developed also to assist small and medium businesses, Large organisations and infrastructure providers as well as Government.
   - The ACSC recommends cloud consumers use Cloud Service Providers and cloud services who are located in Australia for handling their sensitive and security-classified information.

Finland – Finland has in place cloud service guidelines, together with the implementation of Project Cirrus to develop operating models and contract terms for public cloud service.

a. Cloud service guidelines
   - Cloud service guidelines are prepared in accordance with the Ministry of Finance (Ministry of Finance) Decision and promote the use of central government cloud services to support the development of services. The guidelines determine how the services of the central government organisation and the information contained in them can be handled in public cloud services.
   - The information management unit or agency is responsible for classifying the services and the information containing them, and to provide adequate protection in relation to the risks involved, including introducing solutions and managing changes based on a risk assessment carried out. Decisions made by the information management unit or agency must be documented and archived.
   - Key principles and requirements of cloud service guidelines include:

i. Support decision-making in central government and the life cycle management of strategy and services with regards to cloud services
ii. Clarify the required measures for the utilisation of cloud services
iii. Specify roles and responsibilities for the utilisation of cloud services

b. Project Cirrus
Its key objective is to speed up the public sector cloud transition, through creating cost-effective operating models that reduce and eliminate the risks associated with data protection in cloud computing services and meet the requirements of the public sector. In addition, it also provide tools for various data protection, information security and preparedness needs.

Israel – Israel has established a Cloud Center of Excellence (CCoE) to develop the cloud policies for the Israeli Government. The CCoE has published The Israel Cloud Strategy which defines the goals and objectives for the Nimbus Project – a national large-scale initiative that aims to provide comprehensive cloud services to the Government of Israel. Below highlights the key policies in the Israel cloud environment:

- Cloud First Policy where all new applications/programs are to be first analysed for cloud match preferring Cloud Native and SaaS usage wherever possible.
- A policy of a Landing Zone for all applications and workloads with the baseline of all security and policy defined in the government.
- Only information that is not Confidential is allowed to migrate to cloud as of now. A set of rules has been defined that allow ministries to determine the data and system and receive a decision of the security measures needed when migrating to cloud. Moving forward, this is in the process of digitalizing from the decison being made via the cloud committee to a self regulation tool, except in certain cases where the committee will continue to meet.
- Infrastructure as Code is a policy that is enforced with all Managed Service Providers (MSPs) working with Ministries to ensure the ability to automize and manage platform code.
- Have a Cloud Journey methodology that defined at two levels that each agency will set out on – Ministry Journey and Project Journey. Each type defines and explains the stages that must be taken in order to fulfil the journey. This methodology will be used in different stages on assistance given to agencies: for example budgets, training, professional architecture assistance.

New Zealand – New Zealand's Cloud First policy, refreshed in April 2023, recognises the potential of public cloud to deliver better, more agile, innovative and secure services that meet the needs of New Zealanders. The transformation of the public service to a modern, agile and adaptive public service (in line with the Strategy for a Digital Public Service and the Digital Strategy for Aotearoa), can enable people, communities, the economy, and environment to flourish and prosper in the digital era.

The policy reaffirms support for transition to public cloud, and sets the expectation that agencies:

- Adopt public cloud services in preference to traditional ICT systems.
- Not invest in on-premise ICT infrastructure unless specific criteria are met or approved by the Government Chief Digital Officer (GCDO).

- Have a plan for how they intend to use public cloud services.
- Make cloud adoption decisions on a case-by-case basis following a risk assessment.
- Consider Te Tiriti o Waitangi (The Treaty of Waitangi), and principles of accountability, ethics, transparency and collaboration with Iwi and Māori, when making decisions about adopting cloud services, particularly for Māori data.
- Make cloud adoption decisions which consider high-level sustainability principles.
- Only store data classified as RESTRICTED or below in a public cloud service.
- As a preference, over time, host RESTRICTED information in a New Zealand based data centre, where a suitable onshore service is available.

The adoption of cloud is supported by:

- Government Chief Digital Officer (GCDO): The GCDO is the system lead for digital. They are responsible for the development and management of digital for the state sector. This includes development of a common vision for the future, setting standards and frameworks, supporting best practice, and identifying opportunities for inter-agency collaboration. They also lead the development of shared digital process and infrastructure which agencies can then adopt. The GCDO is hosted within the Department of Internal Affairs. The GCDO works closely with other system leads, such as the Government Chief Information Security Officer and Government Chief Data Steward.
- Commercial arrangements, through a range of all-of-government agreements or Cloud Framework/Software Agreements. A new all-of-government Cloud Sourcing Strategy is underway. The strategy will seek to support government agencies to procure a diverse range of secure and resilient cloud services.
- Security guidance and cloud risk discovery tools are available through the GCDO or the New Zealand Information Security Manual (NZISM). This work has included the development of NZISM baseline security templates that help agencies and providers to easily implement some NZISM controls.

Singapore - GovTech Singapore has created Government on Commercial Cloud (GCC). GCC is a "wrapper" platform that provides government agencies with a consistent means to adopt commercial cloud solutions offered by cloud service providers supporting golocal with data residency within Singapore Region. To improve the user experience and ease the adoption of commercial cloud solutions provided by the leading service providers such as Amazon Web Services (AWS), Azure and Google Cloud, GCC 1.0 was redesigned to give rise to GCC 2.0. GCC 2.0 was launched progressively from May 2022 and leverages existing cloud-native capabilities and aligns with cloud security practices. It enables product teams to deliver government digital services more quickly and securely at reduced costs. Singapore's goal is to migrate 70% of the government workloads to commercial cloud by end of year 2023, and currently approximately 60% have moved to the cloud.

Singapore is also constantly evolving our Cloud policies (i.e. Commercial Cloud First Policy). In 2021, further segregation was done for the Confidential classification which created a new Confidential (Cloud-Eligible) level, and this allowed the Confidential (Cloud Eligible) workloads to be moved to cloud.

In addition, Singapore has also launched the GCC+ platform in July 2023 as the central hosting platform for Confidential systems. GCC+ provides hosting on the AWS Private Local Zone (PLZ) and caters to the requirement for data sovereignty and security compliance for Confidential systems.

United Nations – In the UN's shared vision for future global cooperation, "Our Common Agenda", the UN Secretary-General highlighted the Sustainable Development Goals and proposed for a Summit of the Future in 2024 to agree on a Global Digital Compact. Countries are encouraged to invest in digital public infrastructure that must be open, inclusive, secure and interoperable, and to enhance the capacity and skills for all to make full and safe use of digital connectivity.

In the upcoming UN E-Government Survey in 2024 (a biennial publication of UN DESA), a global scan on cloud strategies would be conducted to survey member countries on whether there is a national cloud strategy in place. Initial findings highlighted that cloud adoption varies widely from country to country with many public institutions, in both developed and developed countries, still being skeptical about trusting cloud along with its challenges and risks.

In considering cloud policies, other than aligning with international standards, certifications as well as industry standards, UN also advocated a principles-based approach, including principles like effectiveness, whole-of-government, accountability, transparency, and inclusiveness.
UN DESA also encouraged DGX member countries to share their cloud costing approach, as low- and middle-income countries are faced with greater infrastructure constraints and resource challenges in adopting cloud and benefiting from cloud-enabled e-services.
As part of the ongoing methodology enhancement of the UN E-Government Survey, UN DESA is also exploring the feasibility of introducing a set of metrics on cloud for digital government, consisting of parameters like the enabling environment, sustainability, security, agility, quality, responsiveness, and the reach of cloud-enabled e-services.

Data Classification Framework

5. In general, each member country has its own data classification framework or equivalent, and the hosting approaches are recommended in accordance with the risks and appropriate measures put in place to manage and safeguard data. There is general consensus that the approach for level 2 and below systems are to be hosted in cloud, while level 3 systems would need to be evaluated before hosting in cloud is allowed. Above that, systems which are critical to national security would still be hosted on-premises.

<table>
<tr><th>Classification Level</th><th>Australia</th><th>Finland</th><th>Israel</th><th>Singapore</th><th>New Zealand</th></tr>
<tr><td><u>Level 1</u>
Does not cause damage to agency or national interests</td><td colspan="4" rowspan="2">On Commercial Cloud / Certified Hosting Provider</td><td rowspan="3">May be on public cloud after risk assessment. Decision by agency</td></tr>
<tr><td><u>Level 2</u>
Causes some damage to an agency but no damage to national interests</td></tr>
<tr><td><u>Level 3</u>
Causes some damage to national interests, or serious damage to an agency</td><td>Agency-based risk assessment in conjunction with the</td><td>Private cloud/ on-premises</td><td>Assessment by Cloud Committee on suitability to be hosted in Nimbus</td><td>Confidential (Cloud Eligible) systems hosted on Commercial</td></tr>
</table>

	Protective Security Policy Framework (PSPF) and Hosting Certification Framework		Public Cloud; Else on Private cloud/ on-premises	Cloud; Confidential systems would be hosted on private cloud/ on-premises	

B. Measures to further accelerate Cloud Adoption

With member countries at different stages of the cloud journey with unique circumstances and use cases, various measures are used to tackle a variety of issues.

Cloud Community and Sharing Platforms

6. A cloud community could be setup with representatives from the ministries or agencies to facilitate sharing and learning from each other. In Israel, the Cloud CCoE is the owner of this community, plans community events and helps reach out to its ministries. To address the lack of knowledge in the ecosystem currently, the Cloud CCoE has defined cloud architects as one of the main points of contact with ministries to provide support and guidance for projects, decisions architecture amongst many of the other responsibilities. Currently, two Head Cloud Architects have been drafted into the Cloud CCoE. The Cloud CCoE has also put in place communication platforms for knowledge sharing – (1) Internet website to ensure transparency to its citizens, sharing activities and policies defined for their Nimbus Project, and (2) an internal website for internal policies be shared within the government. In Singapore, regular events engaging both industry and agencies (i.e. Stack-X, Stack Meetup events) also aims to reach out to the community to share the latest technology and roadmap. This promotes networking of experts in cloud and other supporting domains where people could exchange information and learnings points with each other.

Migration Strategies and Playbooks

7. To drive the adoption of cloud, governments may devise **migration strategies, and along with the development of playbooks** to guide ministries or agencies in adopting Cloud. These guidelines could cover the operations model (i.e. Technology, Process, People, Migration processes), as well as best practices in FinOps and Cybersecurity, etc. In Singapore, **central Cloud Adoption Teams (CAT)** are also set up to work and handhold agencies in the migration process. Initial phase of migration is slow with a lot of handholding, but once the ecosystem of supporting vendors is in place, the process became easier and smoother. In addition, there are also regular steering meetings with agencies Chief Information Officer (CIO) to path the way and drive cloud adoption.

Modernisation of IT Policies

8. IT policies needs to be aligned with the push for cloud-native architecture. In contrast with traditional architecture in on-premises setup, the policies would also need to be constantly updated to support the evolving technologies in the cloud. Traditionally, governments would have one set of IT policies to govern all infrastructure requirements. However, with the fundamental change in technology and shared security model in cloud, member countries have echoed the trend that IT policies are being evolved to separately address and tailor specifically to facilitate governments to move to cloud, without needing to comply with requirements that are more applicable for on-premise system.

Training Programme

9. Cloud training programme is important to ensure there is adequate support from the ecosystem with the right skillset to support the adoption of cloud technologies. Multiple domains would need to be reskilled including IT departments, Procurement and Business units to understand and support cloud projects. Conversely, information is also shared with Cloud service providers to assist them in understanding the government eco-system and limitations.

10. In Singapore, **Cloud training programme** not only applies to government officers via Digital Academy but also extended to vendors and industry players via Tech Talks and Trainings, as well as partnership with a local university to manage the cloud space effectively. This include ensuring certifications are in place and working with CSPs on training programmes. There is also a competency framework to enable engineers to reskill.

Procurement Approach

11. Procurement to enable purchasing on cloud marketplace to be more direct, where a separate procurement process is not necessary. In Singapore, GovTech works closely with the Ministry of Finance to help agencies manage the financial aspects of Cloud. For example, with CAPEX shifting to the OPEX model in cloud subscriptions, this results in lack of flexibility on agencies' budget management.

12. In Finland, ICT services are provided by Valtori as the Government ICT Centre. Their services are a combination of in-house and outsourced commercial services by trusted partners. For procurement of cloud services, Nordcloud Oy has been awarded by Valtori as the provider of Microsoft Azure Enterprise Agreement (EA), Amazon Web Services (AWS) and Google Cloud Platform (GCP) services in a framework agreement that is valid for three years.

FinOps

13. Commercial Cloud hosting costs are on a per usage basis, which is different from traditional on-premises costs. From a central perspective, it would be beneficial to maintain an oversight of how agencies are managing costs and help them optimise these costs. Singapore looks at the Cloud FinOps model mainly involving three phases:
    a. **Inform** – Visibility and sense-making of data available on cloud platform, making use of cost management tools, aggregating account level data and insights in order to track for trend analysis, form benchmarks and determine optimization progress and anomalies.
    b. **Optimise** – Cost analysis would need to cater to needs of stakeholders at different levels (i.e. CIOs, project managers, system analysts and engineers). Various cloud native optimisation services could also be used to ingest and automate the analysis to provide for focused cost control and optimisation execution based on contextualised recommendations. Common optimization efforts include removing unused resources, scheduling resources based on needs, right-sizing and adopting of savings plans based on usage trends.
    c. **Operate** – Build a proactive culture around Cloud cost monitoring, management and optimization, including the necessary tools, monthly reports, review forums, initiatives to adopt cost saving solutions (i.e. serverless, scalable architecture), automating trend analysis and anomaly detection.

C. Centralised services as an acceleration to Cloud

14. Providing centralised cloud hosting platform is often not sufficient to drive quick migration and adoption of cloud. Along with the platform, the dependency services should also be provided in

tandem to alleviate pain points and speed up the process. Key central/shared services may also drive behavioural cloud deployment models and influence the development of modernised applications. However, there may be scenarios whereby countries work on a decentralised approach in the building of their systems and services, and the benefits with centralised common services may be limited.

Shared Infrastructure Services

15. In the Israel Cloud Strategy Shared services is a key measure that is defined as a means to speed up the pace of releases and upgrade the technology possibilities allowing ministries to focus on the "main line of business" for the citizens while using shared services defined by and for the government. Key shared services includes the Government Landing Zone as the baseline platform, Data highway as an ApiGateway for data movement, Internal Government Code Share for sharing of solutions and code between agencies, Identity Management as a government federated service, as well as central services like Mail Platform and IT Service Management.

16. In Singapore, providing central services is a crucial measure to support agencies development in cloud. Services such as Identity Services, automated compartment provisioning, development of hosting models, common services like vulnerability management service, centralised logging and monitoring, anti-malware and backup services are being provided centrally.

Sharing of Government Architecture

17. Sharing of IT policies and standards to the ecosystem would make these information available commonly so that the industry is aware of the requirements and be able to support the needs of the community. The Australian Government Architecture (AGA) is a decision-making and policy framework that helps agencies develop scalable, secure, and resilient digital capabilities. AGA provided transparency in sharing the capabilities to be built by agencies and industry. AGA's codification help government agencies classify and assess individual investment proposals about whether they are aligned to government policies and standards. This is to provide a shorthand view of the more complex architectural content.

18. As a key part of Australia's Whole-of-Government Digital and ICT Investment Oversight Framework, the AGA architecture:
    a. Provides guidance to agencies on how to deliver capabilities faster and in a way that is consistent, interoperable, promotes reuse, represents less risk and ensures value for money.
    b. Sets clear signals for industry in describing the way in which capabilities are expected to be delivered.
    c. Supports agency decision-making and creates transparency by publishing standards and patterns for digital and ICT capabilities.
    d. Identifies gaps in capabilities and emerging technology where investment is required.
    e. The architecture establishes the relationship between strategies, policies, and architecture artefacts – providing clear guidance to agencies planning digital investments.

19. To facilitate rapid development and deployment in Cloud, GovTech Singapore also set up the Singapore Government Technology Stack (SGTS) for developers to have a common set of toolchains with proper controls in place to guide developers in developing cloud applications quickly. With SGTS, agencies would be able to tap on a suite of tools and services hosted on a common infrastructure to ensure consistency and high quality of their applications, reducing the time and effort needed to introduce new digital services, enhance and maintain existing ones.

Developer Tools and Support

20. In addition to providing common hosting platforms for agencies in Singapore, GovTech offers a set of common DevOps solutions centrally to support cloud application development across the public sector. GovTech adopts a Cloud-First principle which includes the use of SaaS for easier scale-up and reduction of operational overheads due to self-hosting. The approach is to carefully choose SaaS platforms that are widely used (e.g. Gitlab) in the industry while also selectively integrating best-in-class solutions (e.g. Fortify-on-Demand, Sonatype) for certain areas like code security. By centralizing these toolchain services, the engineering team will be able to leverage on reusable code components to accelerate development and apply checks that helps improve code security. It also allows teams to apply templates that enforce security policies and compliance as part of automation. Inner-sourcing also encourages developers to consume and to contribute useful components within the public sector development landscape by repo sharing and code commit moderations, while GovTech designs the solution for easy discovery to other users. It's also essential for the central solution to provide full visibility on development activities and practices, thus observability metrics were developed as part of the platform to help GovTech drive DevSecOps practices, accelerate development efficiency, and to enforce governance & compliance in a more effective manner.

Annex A :

Additional materials and references may be found below.

Australia

Further references are provided to share more information on the following:

1. Hosting Certification Framework
   Framework | Hosting Certification Framework
   Hosting Certification Framework - March 2021.v2.pdf
2. Anatomy of a Cloud Assessment and Authorisation
   Anatomy of a Cloud Assessment and Authorisation | Cyber.gov.au
3. Digital Sourcing Consider First Policy
   Resources and policies – BuyICT
4. Policy for handling sensitive and classified information
   https://www.protectivesecurity.gov.au/system/files/2023-01/pspf-policy-08-sensitive-and-classified-information.pdf
5. Australian Government Architecture
   https://architecture.digital.gov.au/
   https://www.dta.gov.au/australian-government-architecture

Finland

In Finland, ICT services are provided by Valtori as the Government ICT Centre. More information may be found at the following reference:

- ICT services for the central government | Valtori

Israel

Israel's holistic approach to Cloud in government offers government agencies a full set of tools to implement cloud projects: Starting from two public clouds in Israel that have built the region in accordance to regulation defined by The National Cyber Directorate and The Ministry of Defence, A Cloud Center of excellence to establish policies, guidelines and change management program , a shared service approach to enhance the sharing of code and platforms, a closed set of service providers ready to service government agencies, a full marketplace of solutions of SaaS and Non-SaaS, and service providers to assist in optimizing the Day 2 cloud maintenance.

Israel has put in place the five layers of the Nimbus Tenders built to provide an overall strategy (Israel Nimbus Project) for all government agencies (available also to organizations that take part in the Nimbus Project):

Layer 1	Public Cloud Provider	Two Public Cloud Providers won the tender and are opening a Cloud Region in Israel: AWS and Google Cloud = "Nimbus"
Layer 2	Government Cloud Center of Excellence	A government CCoE is being established and is working on best practices, policies, guidelines, change management, training program, reference architecture, multi-cloud policy.

Layer 3	Service Providers	This tender is an ongoing tender to allow for Service Providers to join the government effort. These Service Providers give the government agencies and offices expertise in a number of cloud domains, such as, automation (IAC), modernization, cloud development, discovery and assessment, workload placement, multi-cloud strategy and more. Using this tender Ministries are able to contact and work with pre-agreed providers to improve and speedup the contract between the ministry and service provider.
Layer 4	FinOps and Optimization Services	This tender is indented to allow Ministries to use pre-agreed provider services to work on optimizing the cloud usage. This is one of the main changes as with the migration to cloud, ministries must be supported on handling the 'Day 2' processes needed.
Layer 5	Government Private Marketplace offerings	The stage after choosing the Cloud Providers in the first tender is to fill the government offices with as many options as possible for Cloud solutions. This is implemented by a tender with pre-agreed terms with the Israel Nation Cyber Division to allow for SaaS and Non-SaaS. The goal is to add hundreds of private marketplace service providers that will allow the implementation of many different high-end solutions in ministries with minimum procurement processes and delays.

Key shared infrastructure services are also in place to accelerate cloud adoption:

a. **Government Landing Zone** is a government platform that implements the security policies at the base level and all ministries that open an account on the Government Landing Zone would inherit all policies. This allows for quicker adoption of cloud with a high level of security and policy.

b. **Data Highway** is an ApiGateway as a central service implemented on the Government Landing Zone allows to securely share data across agencies using policies within the landing zone to speed up the definition process.

c. **Internal Government Code Share** is a new service being defined and checked to be used has a platform to share code between agencies. This is in accordance to the Cloud Strategy to share solutions and code.

d. **Identity Management** is a service planned to be implemented as a government federated service, each ministry will define and manage its users based on a central policy defined top down. This service is now in a tender process.

e. **Mail Platform** is central service planned to be implemented at the National Digital Agency Level and used by all ministries. This service has not been implemented as of current.

f. **IT Service Management** central service to be implemented at the National Digital Agency Level and used by all ministries. This service is in planning and has not been implemented as of current.

References:

- https://www.gov.il/en/departments/news/cloud-first

New Zealand

References:

1. Cloud First Policy: www.digital.govt.nz search 'Cloud Services'
2. New Zealand Information Security Manual (NZISM): www.nzism.gcsb.govt.nz
3. Classification System: https://protectivesecurity.govt.nz/classification-system/overview/
4. Strategy for a Digital Public Service: https://www.digital.govt.nz/digital-government/strategy/strategy-summary/about/
5. Digital Strategy for Aotearoa: https://www.digital.govt.nz/digital-government/strategy/digital-strategy-for-aotearoa-and-action-plan/the-digital-strategy-for-aotearoa/
6. Public Service system leads: https://www.publicservice.govt.nz/system/leaders/public-service-system-leaders/system-leads/

Singapore

References:

- Singapore Government Developer Portal https://www.developer.tech.gov.sg/
- Government on Commercial Cloud (GCC) https://www.developer.tech.gov.sg/products/categories/infrastructure-and-hosting/government-on-commercial-cloud/overview.html
- Singapore Government Tech Stack (SGTS) https://www.developer.tech.gov.sg/singapore-government-tech-stack/
- STACK 2022 – Sharing on Cloud FinOps https://www.youtube.com/watch?v=wCzGgs86I58

United Nations

References:

- Our Common Agenda | United Nations
- UN Policy Brief on Global Digital Compact
- UN E-Government Survey