Building Blocks for a Successful Digital Transformation Strategy

Realizing a Country's True Potential

Microsoft Linklaters

Foreword

The ability to devise public policy frameworks that are agile enough to keep pace with the ever-increasing velocity of technological innovation is an enduring challenge for governments all over the world. Through consistent engagement with policy and procurement stakeholders across the globe, we have observed how governments are navigating the complexities of their unique digital transformation journeys and have developed an awareness of the building blocks necessary to deliver optimal digitization outcomes.

Microsoft, in partnership with Linklaters, has developed this paper with the goal to share these insights, contribute to ongoing dialogue and demonstrate our shared commitment to advance the policy and procurement agenda of governments around the world.

Innovation is at the heart of both our businesses; it defines our objectives and priorities. Therefore, it is our great hope that **Building Blocks for a Successful Digital Transformation Strategy - Realizing a Country's True Potential**, serves as a useful resource for public sector and policy stakeholders who might wish to chart their own course towards sustainable innovation and digital transformation.

Andrew Cooke

Global Policy Lead, Worldwide Public Sector
Microsoft Corporation

Richard Cumbley

Partner
Linklaters LLP, London

This paper was jointly authored by the teams at Microsoft and Linklaters, acknowledging contributions from Amarachi Utah-Adjibola and Joseph Salazar of Microsoft Corporation and Adrian Fisher, Ashleigh Sinclair, Claudia Leong, Evan Chooi, Jia-Yi Tay and Matthew Creagh of Linklaters

Contents

A Introduction

Technology is a proven pillar of competitiveness and growth for governments worldwide. Countries that are able to harness the power of technology, especially new and emerging technologies like cloud computing, stand to increase productivity, foster innovation, and realize cost savings, all whilst better engaging with and supporting their citizens.

As a global company that is committed to empowering every person and every organization on the planet to achieve more, Microsoft's Worldwide Public Sector team has supported hundreds of government customers around the globe and has experience working with a wide array of laws, policies and practices related to technology procurement. In a similar vein, as a global law firm with technology teams in the US, Europe and Asia, Linklaters has supported hundreds of government customers and technology suppliers.

Due to our exposure to contrasting approaches to public procurement around the world, both Microsoft and Linklaters have become a "sensor network" of global public sector best practices. As a result, we are often asked by policy makers, procurement executives and public sector information technology strategists to share our insights on **who is doing it well and why?**.

In the spirit of responding to this complex question, we are excited to share our perspectives on good public sector technology policy and procurement practices.

Getting policy settings "right" is tough, and is best considered a journey rather than a destination. Given that the economic landscape, end-user demands and indeed the technology on offer are constantly evolving, it is essential that policy approaches flex in tandem. One key observation we have made is that policy that does flex and stand the test of time is often principles based, rather than being overly prescriptive. Through a collaborative approach to policy engagement, we truly believe governments can develop the sort of agility that will help to unlock significant opportunity and potential, regardless of where a country is, on its digital transformation journey.

B The Goal of Digital Transformation

Digital transformation is the optimisation of a government's use of digital technologies to streamline, innovate and improve the quality of services for its citizens, as well as to optimise operations, and gain and act on insights from data. A government that is best able to leverage digital services and data will be more agile and resilient.[1] The COVID-19 pandemic showed the importance of this and demonstrated how far many government agencies still have to go to become truly digital-first.[2]

Deloitte suggested in its 2021 paper "Seven pivots for government's digital transformation: How COVID-19 proved the importance of being digital", that governments need to move from doing digital to being digital. In other words, instead of simply leveraging digital technologies to increase capabilities while still relying on legacy operating models, governments need to embed digital technologies and processes into their operations to transform service delivery and back-office-operations.[3]

Research has shown that there is a clear correlation between governments' use of digital technologies and higher growth in Gross Domestic Product (GDP).[4] Therefore, governments that can build digital capacity, will reap the many benefits of digitalization, including service efficiency, productivity, innovation, flexibility and agility, scalability, resilience, data security improvements, and cost-savings.

C The Building Blocks

As a result of our engagement with governments across the globe, we have developed a comprehensive view of the world's public sector technology policy and procurement landscape.

In the context of that engagement, we share the **building blocks** that have, in our experience, proven to be the foundation for successful digitalization of the public sector in the countries that we have worked with. These building blocks are:

1. A national cloud strategy and cloud first policy;
2. A data classification framework fit for the digital age;
3. Adoption and implementation of a digital identity solution;
4. A centralized procurement function;
5. Use of government framework agreements;
6. Flexible and adaptive finance rules;
7. A collaborative approach amongst stakeholders; and
8. A digital culture and technology skilling agenda.

For each of these building blocks we have identified their core components, the key challenges each seeks to address, and how certain countries have implemented these building blocks in practice, usually taking a principles-based approach, applied in a technology or solution agnostic manner, enabling them to flex as the digital transformation offerings themselves evolve.

Importantly, these building blocks are linked; the implementation of one contributes to the implementation and success of others.

Building Block 1

Adoption and implementation of a National Cloud Strategy and Cloud First Policy

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- ✓ No digitalization vision or strategy.
- ✓ Reliance on existing IT services and infrastructure.
- ✓ Expense of digital transformation.
- ✓ Lack of government support.
- ✓ Mistrust of cloud services.

One of the key barriers to digital transformation is the lack of an appropriate digitalization vision and strategy. Often governments are relying on traditional on-premises IT services and/or they are parties to conventional long-term outsourcing arrangements and as such, change is resisted as the status quo is seen as the easier or safer option. Cloud services may be perceived as inappropriately risky and, in less digitally mature economies, the benefits of cloud computing may not be widely promoted or embraced across all levels of government. Combatting this mistrust and misperceptions is a challenge. That's why the use of the cloud should be recognised as both a strategic and technological investment tool for governments via a national cloud strategy and a cloud first policy.

That strategy should reflect the areas where cloud and digital transformation technologies offer obvious advantages: volume flexibility, adaptability to new needs, enabling innovation; improved efficiency and use of resources, potential cost reduction and the removal of unofficial investments in technology; enhancing productivity; promoting collaboration between departments and delivering improved quality of services to citizens. In addition, because payment for cloud services is usually tied to usage, government customers can avoid major investments in capital, budget, hardware, software or installation, as was traditionally the case. Instead, the service is provided by third parties who make the investments spreading capital investment costs across multiple years and customers. Cloud services also help enable governments to meet sustainability goals as, by virtue of their relatively recent creation, hyperscale cloud computing services often consume significant less energy and materials compared to when customers operate an on-premises technology strategy, and embrace the use of renewable energy sources. Microsoft has been carbon-neutral since 2012 and has committed to being carbon negative by 2030.

Using the shared infrastructure of the public cloud also helps government agencies efficiently share data with each other, enhancing collaboration, driving shared value by enabling better – and consistently generated and presented - analytics and insights across agencies and allowing greater flexibility to meet the changing needs of government. Using traditional IT systems, governments often find that data stored by one agency on its own IT system could be inaccessible to other agencies because IT systems are incompatible or are running different or outdated software versions. By consolidating government data in the cloud, sharing infrastructure, and subjecting all data to harmonious technical, operational and data security frameworks (Refer to Building Block 2 (Data classification and security framework)), government agencies can collaborate more efficiently while maintaining the level of security that their data requires.

Governments that use the cloud seek a good balance between the data and services they prefer to manage directly and those that migrate to the cloud, for the benefit of citizens and for efficient public sector activity. All hosting comes with risk and governments will need to decide whether the benefits that the cloud brings outweighs the marginal risk of engaging a third party in a highly interconnected world. An appropriate data classification policy will help assist with this, giving clarity to which data classes can and should be moved to the cloud and which, like highly classified workloads, properly, should not. Refer to Building Block 2 (Data classification and security framework).

A common element of all digital transformation strategies of digitally mature governments or those on the path to digital maturity has been the adoption of a national cloud strategy and a cloud first policy, alongside an appropriate data classification strategy (refer to Building Block 2). This is a government directive, legislation, executive order, or presidential decree, which prompts government agencies to create and execute IT systems in the public cloud as standard or default, other than in respect of the very narrow category of highly classified data that is critical to national security. National cloud strategies and cloud first policies instruct public agencies to prioritize the use of this model when they need to implement digital technologies. They may also require express justification for any IT investment that doesn't involve the use of cloud.

As reflected in national cloud strategies, the importance of using the cloud is not just a technical matter or a measure to save on public spending. For many governments, it is a policy approach that unlocks increased program efficiency, efficacy and improved citizen service delivery. In our experience, the most forward-thinking governments commit to a national cloud strategy and a cloud first policy not just because it brings incremental improvements to their existing IT or data centre approaches, but also because it transforms their IT infrastructure and their ability to provide the best level of services to citizens.

As many governments recognize the benefits of cloud technology, they are implementing policies to encourage its uptake and reap the rewards. In particular, governments are encouraging the use of secure public cloud computing services to deliver the maximum possible computing power, availability and resilience of data and value-for-money. In countries such as the United States, the United Kingdom or Australia, virtually all government agencies use the cloud in some manner. Currently, 90% of OECD governments have decided to achieve the benefits of these technologies and have demonstrated advanced implementation through using cloud technology.[5]

In the next spread, we have set out some examples across the globe showcasing the use of national cloud strategies and cloud first policies, for South America[6] (Chile, Colombia, Brazil, Argentina), Nigeria[7], Singapore[8], Australia[9,10], the UK[11,12,13,14], Canada[15,16,17] and the USA[18,19,20,21].

South America

The below showcases governmental support of prioritisation of cloud services although, their effective implementation remains varied:

- In **Chile**, an executive directive was signed by the Presidency to create a cloud first policy.
- In **Brazil**, the Ministry of the Economy has issued a binding directive for executive bodies to operate a cloud first policy. However, the directive is not binding for other branches (legislature and judiciary) or at the state level, and a higher political instrument may be needed in the future.
- In **Argentina**, the Decálogo Tecnológico of August 2018 prepared by the National Office of Information Technologies (ONTI) instructs the federal government to prefer cloud solutions. However, complementary, more detailed, regulations are still under development.
- In **Colombia** the National Development Plan of the Iván Duque Márquez government contained in Law 1995 of 2019 clearly establishes the need to prioritize cloud services for the optimization of public resources and advancement in the digital transformation of the country, incorporating technologies emerging from the Fourth Industrial Revolution. The National Congress approved a Cloud First Policy, which was subsequently sanctioned by the President.

Nigeria

The Nigerian Government has shown its commitment to fostering the growth of the local ICT industry, improving business continuity and quality of service delivery in the public sector by its adoption of a "cloud first" policy in 2019. This applies to all federal public institutions, public institutions at state and local government levels and corporations fully or partially owned by the Federal Government in Nigeria. The goal is to ensure a 30% increase in the adoption of cloud computing by 2024 among federal public institute and SME that provide digital-enable services to the government.

Australia

The Australian government released its updated cloud first policy, the Australian Government Cloud Computing Policy – Smarter ICT Investment, in October 2014. This policy reframed the implementation of cloud as being mandatory, where it is fit for purpose, provides adequate data protection, and delivers value for money.

The Australian government further introduced the Secure Cloud Strategy in 2017 (which was updated in 2021). Under this strategy, agencies develop their own cloud strategies to suit their own needs, with guiding principles around security, hosting and data considerations. The Digital Transformation Agency has emphasized in the strategy that digital transformation and innovation is crucial to Australia's economic prosperity.

Canada

In Canada, the province of Quebec used its authority to announce a Cloud First Policy.

The Government of Canada's Cloud Adoption Strategy also focusses on the cloud being the preferred option for delivering IT services, with public cloud being the preferred option (previously it had a "right cloud adoption strategy").

United States

The US has a federal "Cloud Smart" strategy which builds on its original cloud first policy and provides more guidance in respect of security, procurement, and necessary workforce skills to foster cloud adoption and implementation.

The US has a number of success stories of successful cloud implementation across its government departments, including:

- **US Agency for International Development:** USAID uses cloud technology to overcome the security vulnerabilities from operating in low network connectivity bandwidth environments. Since 2018, USAID has used a hybrid cloud solution as part of its Enterprise Data Centre/ Disaster Recovery (EDC/DR) solution. USAID uses multiple data centres to avoid reliance on a specific geographic location, and is 100% cloud-enabled, with no remaining legacy systems. This has led to 30% reduction in costs for operations and maintenance.
- **National Oceanic and Atmospheric Administration:** NOAA uses cloud computing technology in its Big Data Program to facilitate taxpayer access to institutional knowledge about the oceanic and coastal climate and weather. NOAA's Cloud Initiative: (i) uses multiple cloud service providers to avoid becoming locked in to one vendor; (ii) shifts the responsibility onto vendor companies to prepare Statement of Objectives documents, therefore soliciting companies based on their capabilities and removing the need for NOAA to prepare Statements of Work; and (iii) specifies the desired contract type to simplify pricing negotiation.

United Kingdom

The UK government introduced a public cloud first policy in 2013. The key hallmarks of this are:

- Public cloud is preferred over private cloud.
- Potential cloud solutions need to be fully evaluated when procuring new or existing services. This is mandatory for central government and strongly recommended for the wider public sector.
- Departments are free to choose an alternative to the cloud but need to demonstrate that it offers better value for money.

There are multiple success stories of successful implementation of the cloud first policy. Some of these are set out below:

- The **Home Office's** Immigration Technology department reduced its cloud costs by 40% by using a variety of optimisation techniques across storage, use and resources.
- Following extensive damage after flood and fire affecting the **Food Standards Authority's** data centres, it migrated all data and hosting services to the cloud to prevent reoccurrence of such incidents. The FSA now has more resilient infrastructure and data that is more secure. Other benefits include overall savings of 10% (including for the IT budget and equipment) and allowing flexibility to work from home.
- The **Welsh Government** migrated their technology systems, services and data to the cloud between 2016 and 2019. A multidisciplinary team (business and change management, digital and communications staff – see Building Block 8 (Promotion of a digital culture and civil servant upskilling)) was created. The planning and prioritisation process was key and included how to deal with legacy technology and the migration of data (at least 33 million documents). The project was successfully completed with services functioning as intended. The Welsh Government is saving money and benefiting from staff efficiency.

Singapore

The Singapore government has stated that it is ‘doubling down’ on its cloud-first efforts to better develop ICT systems on the cloud and help the government deliver more agile digital applications and services for its citizens.

As part of its Smart Nation strategy, the Singapore government announced in 2018 that it aims for at least 70% of its eligible government systems to be on the commercial cloud.

Since then, more than 150 systems classified “restricted” and below have been moved to the commercial cloud. In 2020, more over S$870 million of contracts were earmarked to double the number of systems on the commercial cloud.

This approach enables the Singapore government to connect separate government agencies with a platform of ready-made cloud solutions so that development and delivery of digital applications is expedited. Some success stories of cloud implementation include:

- Updating the Inland Revenue Interactive Network (IRIN) which is the main infocomm technology system that underpins Singapore’s tax administration and revenue collection service. The redeveloped system simplifies the submission process for individual and corporate taxpayers.
- Launching the Infocomm Media Development Authority’s Integrated Regulatory Info System (IRIS) which enables industry players to make digital submissions of content for classification.
- Installation of smart water meters in by the Public Utilities Board, which enables wireless household water usage readings.

Building Block 2

Data classification and security framework

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- ✓ No standardised classification system, or over-classification of data.
- ✓ Tension with existing regulatory frameworks.
- ✓ Security concerns around movement of data to the cloud.
- ✓ Lack of data sharing across government agencies.

One of the tools that greatly assists with the shift from the exploration of the cloud to deploying the cloud at scale, is an appropriate data classification framework fit for the digital age. Such a framework allows public sector authorities to assign relative “values” to the data they maintain and then manage that data based on its type or characteristics, as opposed to treating all data the same way.

One of the key concerns we hear from governments with moving data to the cloud is security. Data classification is often done hand-in-hand with articulating the security requirements that are appropriate for managing data types. A conformed, simplified and well-documented data classification framework can be an important starting point for public sector entities as they move to the cloud, as it ultimately enables individual decision makers to understand better what types of data can be stored on which type of system. Even governments that are enthusiastic adopters of public cloud services will naturally have questions about moving their most highly classified data to third party operated cloud services. Governments have legitimate sovereignty interests in relation to some categories of secret and top secret data, where the disclosure, lack of access or compromise of such data could lead to loss of life or even threaten national security. For these limited types of data, governments might legitimately decide that it is less appropriate to utilise standard public cloud services, rather they may decide to look to hybrid offerings or cloud offerings that have sovereignty controls or features built in or even retain some conventional hosting capability for this asset class. In the context of a government’s all-up data estate, highly classified data (which usually consists of top secret, military, intelligence or similar state secret information) makes up only a very small proportion of overall government data. There are vast amounts of data which can be (and is) safely entrusted to cloud service providers by government agencies, and having a data classification framework which includes practical guidance and flexibility, is entirely advantageous in this regard.

We understand crafting and implementing a data classification framework fit for the digital age isn’t easy, and we suggest that it should be an iterative process, that builds in flexibility and is principles based. Such an approach helps governments overcome what is sometimes seen as “inflexibility” of a classification framework.

Classifying data into categories allows governments to better protect information and importantly allows them to make informed decisions about accessing, storing and transmitting data. Data classifications done well achieves better results for government agencies, clarifying the safeguards needed to protect different types of information, enabling governments to take a pragmatic approach to the adoption of technology, which in turn reduces uncertainty, standardizes access and reduces costs. For example, while it is difficult to formulate an exact cost comparison, our conservative calculations suggest there is at least a 10x cost difference between the systems that would be required for the most highly classified information a government holds and the commercial systems that are suitable for a range of other government information. For a government’s most highly classified information, there is no doubt that such costs are worthwhile and it may well be that governments are currently unwilling to experiment with new technologies like public cloud computing for such information.

Having a robust but flexible, and principles based data classification framework also fosters greater intra government collaboration (a concept explored in Building Block 7 (The importance of a collaborative approach between different parts of government, and between government, regulators and/or the private sector)), optimal data sharing and enhanced service delivery across government agencies, by allowing them to better aggregate, use and manage data in accordance with its classification. Furthermore, having an appropriate data classification policy prevents a siloed or disaggregated approach to data and information security more generally.

Operationalising classification of data is not without its challenges. There is often a tendency for classifications (and the control requirements of such classification) to be overly conservative and place too much data in the "highly-classified" category, therefore imposing restrictive conditions that may mean losing out on the benefits of public cloud services. Classifications may also be overly-broad, so that data of different risk profiles are grouped and treated together. Over-classification and overly-broad grouping leads to unnecessary costs being incurred.

For this reason, data classification should not be viewed in isolation. Data classification is not just a security question, rather, classification needs to be infused within the national technology agenda requirements, good security principles and also broader objectives around IT modernization, cost savings and improved service delivery to citizens, to achieve a balanced, pragmatic and flexible classification schema. As stated, while not a gating function to the use of cloud, data classification goes hand in hand with national cloud strategies and cloud first policies and requires input not just from IT security experts in government but also decision-makers driving IT and government service reform measures.

Once generated, data classification frameworks need regular review to ensure they continue to meet the requirements of government.

A review of several national data classification frameworks provides some helpful guidance to countries that are looking to guide their public sector authorities safely and responsibly to the cloud including:

1. There is increasingly a link between cloud first policy objectives and updating data classification to ensure long term government cloud objectives can be met, particularly those related to cost.
2. The trend is toward fewer classification categories. Three categories have emerged in some leading countries like the UK and Australia. However, we think there is likely merit in exploring slightly more classification categories – four or five for example - as a reduced number of categories leads to certain categories being overutilized or underutilized, often tending towards greater caution than is necessary or economically advantageous.
3. Practical guidance on how to apply the data classification is essential to ensure front line civil servants don't consistently over-classify data and undermine cloud first policy objectives.
4. The requirements set by different data categories need, where possible, to be technology neutral and principles based. Where possible, setting out the outcomes that must be achieved in respect of each category will make the categories more robust than imposing technology prescriptive requirements that can often be circumvented thoughtlessly.

As follows, we have set out some examples from across the globe showcasing different data classification strategies by governments in the UK[22,23,24,25], the US[26,27,28], Australia[29,30], and Canada[31].

United Kingdom (Three tiered data classification system)

The UK has a three tiered data classification system (previously it had 6 levels), which identifies and values data according to its sensitivity. There are distinct security arrangements for each.

- **Official:** Can be managed with good commercial solutions that mitigate the risks faced by any large corporate organisation. This is the majority of information that is created or processed by the public sector (e.g., routine business operations and services). **Around 90%** of government business will be marked as Official.
- **Secret:** Typically requires bespoke sovereign protection. This is very sensitive information that if compromised could seriously damage military capabilities, international relations or serious crime investigations.
- **Top Secret:** Typically requires bespoke sovereign protection. This is the government's most sensitive information and if compromised could cause widespread loss of life or threaten national security.

The previous six tier data classification system was seen as outdated and not fit for the digital age. The change in data classification has enabled the development of security protections comparable to those of leading private sector companies, saving the UK government billions of dollars in simpler and more effective governance.

In addition, employees from different departments began sharing data (for example, classifications in the Ministry of Agriculture and the Ministry of Health were no longer different, allowing employees to work together appropriately).

The Minister for the Cabinet Office Francis Maude summarised the shift nicely at the time:

"We have changed a security classification system that was designed decades ago and introduced a new system fit for the digital age. It will make it easier to share information and save money. There has been a tendency to over-mark documents rather than to manage risk properly. The most important and sensitive materials must continue to be protected as 'Top Secret' or 'Secret' but for other information the new 'Official' category, with its emphasis upon personal responsibility and accountability, will be appropriate for most of what government does."

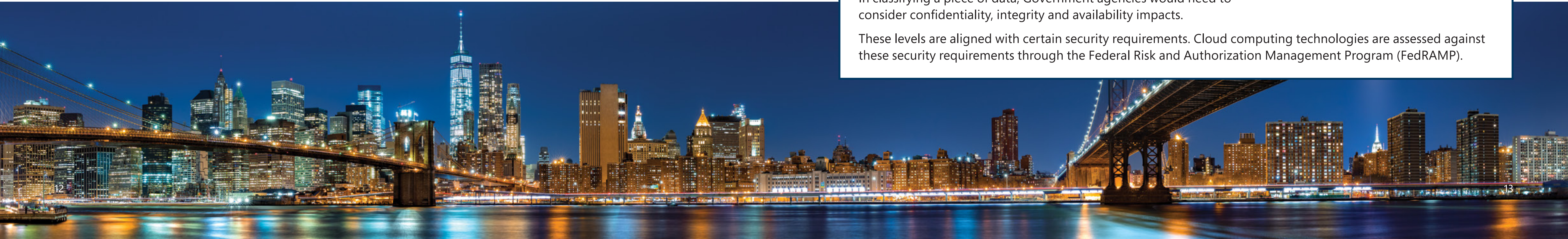
United States

The U.S. National Institute of Standards and Technology (NIST) is a non-regulatory government agency that has released three impact levels for the purpose of classifying data.

These levels correspond to the potential impact on organisations, assets, or individuals in the event of a security breach. Accordingly: (1) "Low" impact means the breach "could be expected to have a limited adverse effect"; (2) "Moderate" impact means the breach "could be expected to have a serious adverse effect"; and (3) "High" impact means the breach "could be expected to have a severe or catastrophic adverse effect."

In classifying a piece of data, Government agencies would need to consider confidentiality, integrity and availability impacts.

These levels are aligned with certain security requirements. Cloud computing technologies are assessed against these security requirements through the Federal Risk and Authorization Management Program (FedRAMP).



Australia

The Australia classification system splits government data into three security classifications, based on the likely damage to national interest, organizations or individuals resulting from compromise of the information's confidentiality:

- **Protected:** information that "could be expected to cause damage".
- **Secret:** information that "could be expected to cause serious damage".
- **Top Secret:** information that "could be expected to cause exceptionally grave damage".

This is encapsulated in the Protective Security Policy framework which was published in September 2018. The framework streamlines the previous data classification method which had more classification categories.

Currently, "protected" data is certified for public cloud.

Canada

In Canada, the federal government went through a data classification process in support of an open data initiative. The first time they had to go through the process, agencies reported that 55% of all data was so sensitive that it could not be identified. After one year of study and training of senior leaders, this number fell to 8%.

Building Block 3

Adoption and implementation of a digital identity strategy

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- ✓ Lack of data sharing and collaboration.
- ✓ Multiple ID's required by citizens.
- ✓ Reliance on hard copy ID verification methods.

The introduction of a digital identity strategy is an important component of digital transformation, in fact it is hard to imagine a public sector digital first world without the effective adoption of a digital identity platform, underpinned by appropriate digital identity operational policies. Given the technology that powers digital identity, it goes hand in hand with the activation of a national cloud strategy and a cloud first policy (see Building Block 1 (Adoption and implementation of a National Cloud Strategy and Cloud First Policy)).

As the world becomes increasingly digitized and many everyday services move online, traditional hard copy methods of identity verification are, in many cases, no longer fit for purpose. Purely online services dealing with hard copy verification solutions struggle with paper complexity, cost and a poor end user experience.

There are much-discussed economic benefits to digital identities. The McKinsey Global Institute estimates that the widespread use of digital identities could unlock economic value in the UK equivalent to 3% of GDP in 2030 through enabling individuals to make increased use of financial services, improving access to employment and creating time savings.[32] The same report also identifies the potential benefits to government as a result of greater employment, reduced fraud and increased tax collection.

As noted in a 2019 PwC report, a single digital identity has the potential to significantly improve citizen experience and convenience by making a wide range of digital services accessible in a seamless fashion.[33] That said, there are also risks that needs to be managed, including technical failures or malicious acts.[34] The McKinsey report notes that careful system design and well-considered government policies are needed to mitigate risks and successfully implement a digital identity strategy and solution.[35]

The introduction of a digital identity strategy and solution needs to be considered through the lens of a country's legislative requirements (including protection of personal data), which are likely to have been drafted at a time when digital identities were not envisaged. In many cases, some form of physical identity document or in-person verification may be required to comply with current law. Accordingly, new primary legislation or amendments to existing legislation may be needed, much in the way that laws were revised to facilitate the use of electronic contracts and electronic signatures.

It is not possible to identify the legal impediments to implementing digital identities, or their preferred solutions, without identifying the delivery option to be implemented. Delivery options, impediments and potential solutions to those impediments are all bound together. As a result, the potential regulatory and complaints handling models and data protection solutions will vary depending on the delivery option adopted.

The availability and affordability of digital ID technology makes it possible for some emerging economies to bypass more traditional paper-based identification methods.[36] Even more developed economies, which may also have multiple digital identity solutions, are looking to create a single identity solution for reasons of scale, and to overcome data silos.

In the next spread, we have set out some examples from across the globe (Italy[37], Singapore[38], UK[39], Estonia[40,41], Canada[42,43,44,45] and India[46,47]) showcasing the shift to a single digital identity solution.

Italy (Sistema pubblico di identità digitale or "SPID")

SPID allows citizens to access the online services of Italian public administrations with a single, secure and protected digital identity. It can be requested by any Italian citizen, as well as anyone with a valid Italian identity card and fiscal number, who is at least 18 years of age.

All public administrations must make their online services accessible through SPID. However, private companies can also make their online services accessible through SPID, in order to facilitate and simplify the use of their digital services.

A SPID identity can be issued by multiple identity providers, namely private entities such as Aruba, Infocert, Intesa, Namirial, Poste, Register, and Tim which are all accredited by the Agency for Digital Italy (Agenzia per l'Italia Digitale or "AgID"). These entities provide digital identities and manage user authentication in line with the rules issued by AgID.

Singapore (Singpass - National Digital Identity)

'National Digital Identity' is one of the strategic national projects of the Singapore government. This involves issuing Singaporeans and residents with a single digital identity which they can use for both government and private sector transactions. NDI is built on public key infrastructure (PKI) cryptographic security techniques, and the services have been gradually deployed since 2017.

NDI brings together various digital initiatives like the SingPass app, MyInfo and MyInfo Business together to provide greater online convenience and transactional security for citizens and businesses. As of 2021, there are over 4.2 million users of Singpass; this covers approximately 97% of Singapore citizens and permanent residents aged 15 and above.

United Kingdom (Introduction of digital identity legislation)

In March 2022, following public consultation, the UK government announced that it will introduce legislation to ensure digital identities are as trusted and secure as paper based forms of identification (e.g., passports and driving licences).

The Office for Digital Identities and Attributes will be established and act as the interim governing body for digital identities. The Office will have the power to issue an easily recognised trustmark to certify digital identity organisations that meet the required security and privacy standards for handling personal data.

The government has recognised a number of benefits with digital identities including:

- reduction in time, effort and expense attributed to sharing physical documents when individuals need legal proof of who they are; and
- help tackle fraud (in the year ending September 2021 there was an estimated 5 million fraud cases in England and Wales) by reducing the amount of personal data shared online.

Digital identities will not be mandatory.

The importance of collaboration and transparency is key to successful implementation of digital identities. Sue Daley, Director for Technology and Innovation, techUK, has noted "Given the next steps now being taken, continued cooperation between industry and government remains the best chance for a successful implementation of a digital identity ecosystem in the UK. However, we must also ensure we bring citizens on this journey with us: building public trust and confidence in Digital ID must be a key priority as we move forward."

Estonia (e-ID)

Estonia is said to have the most highly developed national ID card system in the world. All Estonians have a state-issued digital identity. It is much more than a photo ID as it provides access to all of Estonia's digital services. Some of its uses include: national health insurance card, proof of identification when logging into bank accounts, digital signatures, voting and submitting tax claims.

In addition to having the necessary technology and infrastructure, other key aspects to the e-ID's success are:

- **Regulatory environment:** Estonian's e-government ecosystem is heavily regulated by legislation that is designed to work seamlessly with Estonia's digital solutions. For example, legislation obliges all Estonian authorities to accept qualified electronic signatures as equal to a hand written signature, stamp or seal.
- **Private sector buy in:** Citizens first saw the value of digital ID by using it for their online banking. Banks did not have to develop their own ID systems and this saved on costs. In addition, Estonia has X-road, which is a data exchange layer that allows the public and private sector to securely exchange data and to ensure data is up to date.

According to a PwC paper, Officials in Estonia report over 1400 years of working time and 2% of GDP annual is saved through its digitized public services.

Canadian province of British Columbia (BC Services Card)

British Columbia first issued the BC Services Cards in 2013. The Cards originally acted as a physical form of government-issued ID, permitting access to services like health insurance with increasing security and privacy for personal identification purposes.

Since then, BC have sought to expand the scope of the card to make it closer to a digital ID, including by introducing an app which allows users to access government services via authentication methods already on any app-enabled devices, such as biometric fingerprint identification on a smartphone, removing the need to use a physical card altogether. Among other services, the app currently permits users to: access health information and medical results, renew car insurance, apply for student loans, register businesses and make filings, and view and manage taxes and benefits. The Card is a key player in the way that BC collects, accesses and shares personal data amongst departments.

Developments in British Columbia may be used as a successful example by the federal government as it continues to explore introduction of a digital identity system across Canada.

India (unified nationwide ID system - Aadhaar)

The Indian government established the Unique Identification Authority of India (UIDAI) in 2009 to create a unified nationwide ID system called Aadhaar, and enacted the Aadhaar Act in 2016 to empower UIDAI in the digital ID system implementation. While the use of Aadhaar for identification is not mandatory, the India government has made it mandatory for using Aadhaar to access government services. The Aadhaar system has helped the India government to improve its efficiency and reduce fraud, e.g. it facilitates the establishment of "e-KYC" system that enables financial institutions to identify customers' digital identification.

There are over 1.3 billion Aadhaar generated, and over 11 billion eKYC transactions performed using Aadhaar.

Building Block 4

A centralized procurement function / central purchasing entity

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

✓ Cloud seen as expensive and individual departments/agencies have their own budgetary constraints.

✓ Individual departments and agencies have their own preferred existing vendors, existing technology solutions and different technology needs.

✓ Opaque spending and procurement across departments/agencies.

Often government departments or agencies have different views on digitalization, different budget constraints, a range of existing individual vendors and different technology needs. These challenges are often cited as reasons for maintaining a decentralized procurement approach that places the procurement function closer to the needs of the final user. However, this decentralized approach can hinder a country's ability to fully embrace the benefits of digital transformation. A centralized procurement model has several benefits, including:[48]

- economies of scale - volume purchases make it possible to obtain significant cost savings and/or receive better services at lower cost;
- standardization of terms across government – this not only contributes to cost reduction but also allows a greater use of shared resources on the government side to manage those terms. In other words, five bespoke contract management regimes providing five bespoke services are significantly more expensive to manage than one contract providing one standardized service using one standardized contract management regime;
- technology harmonization across departments, including the ability to establish a single set of technical and environmental standards;
- the encouragement of transparent governance, including proper recording of transactions, effective management controls, and audit trails;
- greater attention can be devoted to management of contract issues and problem resolution (e.g., service issues) rather than process; and
- human resources are easier to manage – a dedicated procurement team results in clear lines of responsibility, fewer people need to be trained and the expertise of specialist purchasers can be utilized to their full extent.

For these very reasons, there has been a growing trend in government departments and agencies to move away from operating and managing their own IT infrastructure. In parallel with this move, the benefits of a centralized procurement function are being recognized and governments are aggregating their purchasing decisions and acting as large purchasing customers of IT solutions. Cloud technology and digital transformation provides the government with a further "moment" to make this move.

In many jurisdictions (some of which are explored below), governments have established one central purchasing entity to represent the collective needs of government departments, ministries and agencies. By laying down an appropriate framework, principles and standards, a centralized procurement function can assist government to buy cloud services and digitally transform. The move to flexible cloud services will typically provide cost savings over equivalent fixed infrastructure, but the aggregation of procurement of cloud services can provide still further cost savings as well as facilitate greater cross-department collaboration and data sharing.

Centralized procurement of IT services is not the end of the story though. Centralized, single, framework arrangements for IT services can have their value undermined if the process for individual departments to order services under that framework is too complex. We have seen examples where the local ordering under a centralized framework contract is complex, and allows more variation and bespoke arrangements, than a typical standardized arrangement. As a result, in the most streamlined examples of centralized procurement, government makes available centralized procurement of IT services via a simple to use, online sign-up process or portal. These portals allow flexible ordering of services without the complexity of highly bespoke 'call off' contracts, service orders or similar. A number of countries (including the United Kingdom[49], Australia[50], Canada[51], Italy[52], Mexico[53], Brazil[54] and Rwanda[55]) have established digital marketplaces whereby the public sector can procure services for digital projects.

Examples of the central procurement of digital services in the UK[56,57,58,59], Canada[60,61], Australia[62,63] and Singapore[64,65] are set out, as follows:

United Kingdom (G-Cloud)

The UK has a centralized procurement function (Crown Commercial Services) that is responsible for managing procurement (including the central government framework agreements (see Building Block 5 (Use of whole of government framework agreements)). Public sector employees have access to a Digital Marketplace (managed by the Government Digital Services), which, depending on the relevant framework agreement (between government and supplier), is used by the public sector organization to purchase various digital services.

One example is the G-Cloud program. After completing an internal approval process, government officials can procure short-term, pay as you go, cloud services, including IaaS, PaaS, or SaaS. The benefits of the G-Cloud include access to over 38,000 services and over 5,200 suppliers; scalable services; access to latest technology; quick and easy procurement; and reduced costs.

Suppliers needs to apply to sell services under the G-Cloud framework and there is a tender process.

Canada (Shared Services Canada)

Shared Service Canada (SSC) is an agency responsible for delivery of digital services to Government of Canada organisations.

SSC has established:

- strong procurement governance and oversight focused on reviews of procurement activities to make sure rules, policies and laws are followed;
- a strong challenge function to validate technology decisions and ensure negotiators are well equipped when negotiating large contracts; and
- strategies to maximise the consolidation requirements for similar or the same equipment to drive better volume discounts; and agile procurement vehicles to increase procurement activity efficiency.

In March 2022, SSC launched a simplified approach to IT procurement which makes it easier for businesses of all sizes to compete for government contracts (Agile Procurement Process 3.0).

Australia

Australia's Digital Transformation Agency has streamlined its digital sourcing process by consolidating its Digital Marketplace with the BuyICT platform, so that all types of ICT procurement are now in one place.

Australia also updated its Digital Sourcing Contract Limits and Reviews Policy in 2020, which is part of the Digital Sourcing Framework regulating non-corporate commonwealth entities' digital sourcing contracts. The update permits extensions for up to 3 years (instead of being capped at the initial term) and also ensures that performance and deliverables are reviewed prior to any extension.

Singapore

In 2001, the Singapore government set up GeBIZ, which is a one-stop e-procurement portal for suppliers to access government procurement opportunities online.

The Government Technology Agency of Singapore also spearheaded innovative partnership models in 2019 including opportunities for vendors to co-develop solutions with the government (instead of outsourcing), dynamic contracting points (instead of a single point of entry at the start of a contract), and hosting an open innovation platform to lower the barriers to entry for certain collaboration opportunities with the government.

Building Block 5

Use of whole of government framework agreements

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- ✓ Inconsistent terms with vendors across government departments/agencies.
- ✓ Lack of central oversight in respect of: (i) spending and (ii) the digital services already procured by other departments/agencies.

The use of whole of government framework agreements is widespread across digitally mature governments. In fact, 70% of OECD countries have some form of framework agreement for using cloud-based technologies.[66]

OECD Countries with Public or Private Cloud Framework Agreements[67]

Countries with an agreement: 26

- Germany
- Australia
- Austria
- Belgium
- Canada
- Chile
- Colombia
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Hungary
- Iceland
- Ireland
- Israel
- Italy
- New Zealand
- Norway
- Poland
- Portugal
- Sweden
- United Kingdom
- United States
- South Korea
- Switzerland

Countries without an agreement: 11

- Spain
- Japan
- Netherlands
- Slovakia
- Greece
- Lithuania
- Latvia
- Luxembourg
- Mexico
- Slovenia
- Turkey

Notes: The contracts mentioned are those in force from 2018. A cloud framework agreement is considered when a government enters into a centralized contract with one or more providers to provide its dependent entities with some type of infrastructure (IaaS), software (SaaS) or technological platform service (PaaS).

The use of framework agreements has many benefits over traditional procurement models, including: (a) a simplified procurement process which reduces transaction costs and shortens the timeframe for obtaining services; (b) cost savings with lower prices when compared to individual bidding processes; (c) better technical and commercial terms which apply regardless of an individual department's negotiating capability; (d) greater transparency and concentration of information, which helps to control expenses and evaluate supplier performance; (e) a reduction in risk of corruption, with more diversified decisions which impedes contract manipulation; and (f) greater effectiveness at incorporating key terms, such as sustainability commitments.

Framework agreements guarantee neutral access to the entire available supply and allow permanent access to a wide menu of innovative solutions to carry out public service transformations.

Framework agreements tend to be structured as a main agreement between the entity representing the government and the relevant supplier, and at times with call-off terms with individual departments. Framework agreements also have a common set of components, including description of services offered, service standards, security and privacy provisions, price setting and dispute resolution mechanisms. Framework agreements will differ between countries to respond to different objectives, size and institutionalisation of governments and features of different national markets (including the regulatory environment).

In our experience, the following learnings can be taken from countries who have implemented framework agreements for procurement of digital services:

- better results are obtained with framework agreements that operate alongside an advanced procurement system, ideally a centralized procurement function.
- how standardised orders are placed under framework arrangements is an important area to get right: too much flexibility, allowing different parts of government to obtain wide ranging contractual modifications, undermines – even neuters – the benefits of framework arrangements and centralized procurement (see Building Block 4 (A centralized procurement function / central purchasing entity));
- electronic procurement platforms that operate in conjunction with the framework agreements are useful. The World Bank has developed a tool to collaborate with governments in the digital transformation of their contracts (available at eprocurementtoolkit.org);
- having an open data policy with information about the bidding processes and contracts under a standard disclosure scheme is helpful. This will contribute to transparency and evaluation by citizens, the press, research centres or any interested party. The Open Government Partnership (OGP) has developed a set of standards that governments can follow to keep their information open to society (opengovpartnership.org); and
- there is a need for employees specialised in contracting and with the knowledge necessary to compare offers and establish the individual call off contracts of a framework agreement.

A few specific examples of the use of framework agreements in Italy[68], the UK[69,70,71,72], and Australia[73,74] are set out, as follows:

Italy (Consip)

Italy has a specialized public body called Consip, organized as a corporation whose ownership is one hundred percent of the Ministry of the Economy and Finance. According to a Microsoft paper from 2020, at that time Consip manages purchases for the Italian public administration totalling approximately USD 13,000 million annually, the result of 127 different framework contracts, generating an average savings of 20% compared to traditional bids.

Each framework agreement is designed to meet a segment of requirements of public entities, allowing the expansion of the supply of pre-negotiated goods and services offered to them. There are four models used:

- **Convenzioni:** These are framework agreements of goods and services in which all conditions are fully specified and pre-negotiated, granting each item of the contract to a single supplier. Agencies only issue purchase orders without major modifications.
- **Accordi Quadro:** These are recurring goods contracts, not necessarily standard, in which not all commercial or technical conditions are specified, and one item can be pre-awarded to more than one supplier. Thus, entities can generate additional specifications or perform mini-bids between pre-awarded suppliers.
- **Public Administration Electronic Market:** This is a digital catalog of goods and services that aims to facilitate low-value purchases by public entities. These are contracts with a fixed number of suppliers for each product category, in which the technical and commercial conditions are fully specified. However, agencies are free to directly award the offer of a particular supplier, request additional specifications or organize mini-bids among those awarded.
- **Public Administration Dynamic Purchasing System:** These are agreements to which suppliers may accede at any time, provided that they meet the conditions required. There is no fixed application period, which is why they are called dynamic. The objective is to collaborate with the simplification of individual proposals for public entities, in categories of goods and services that are not necessarily standard. Suppliers are pre-qualified and only some commercial and technical conditions are pre-established, facilitating the subsequent bidding processes of each entity.

United Kingdom

The UK government has signed framework agreements with key technology suppliers allowing public entities of the central government to meet their technological needs by having access to the best prices. It has a Digital Marketplace through which the public sector can access and purchase services. There are three framework agreements all managed by the Crown Commercial Services. The Government Digital Services manages the Digital Marketplace.

- **Digital Outcomes and Specialists framework:** For the development of solutions or consulting on specific aspects, such as operations, migration, auditing, application quality testing, and user testing etc. Its specifications are partial and basically define the services in general and the rules for their execution, in addition to pre-selection of a group of suppliers based on their experience. At a second stage, entities define their specific requirements and budgets and request a selection process through shortlisting. The call for this contract is made periodically, every 9 to 18 months, a period in which the agreement remains closed with the pre-selected group.
- **Crown Hosting Data Centres framework:** A long-term framework agreement for the provision of technological infrastructure services (IaaS) and other related services. It follows a provisioning model similar to the private cloud, with flexible and scalable services and pay-per-use. The contract specifications are very complete, as they define the services in detail, in addition to technical conditions, such as service level agreements (SLAs) and commercial standards and conditions, including definitions for pricing. The model also features security certifications made by government agencies for application management and confidential information.
- **The G-Cloud framework:** (see Building Block 4 (A centralized procurement function / central purchasing entity)). A closed framework contract with hundreds of suppliers that offer their cloud solution services, whether IaaS, SaaS or PaaS. It contains details of most of the technical and commercial conditions for pricing. Agencies can compare offers, but not negotiate new prices with suppliers, making their selection based on the technical and budget adjustment criteria, and not just based on price. The call for this contract is made periodically, approximately every 12 months. G-Cloud is currently in its 12th version, with the replacement version 13 expected to be awarded September/October 2022.

Australia

Australia’s Digital Transformation Agency manages the whole-of-government deals on behalf of the Australian government to simplify the procurement of ICT products and services that are in common use across the government. These arrangements aggregate many contractual arrangements into one single deal which is negotiated between the government and the supplier.

This prevents having multiple contractual arrangements with the same supplier for the same goods and services, but with different terms, conditions and price across different agencies. Currently, the government has established whole-of-government arrangements with eight digital service providers, including Microsoft.

Agencies do not have to use any of the suppliers under the whole-of-government framework agreements, but if they select any of those providers, they have to do so under the relevant whole-of-government arrangement.

Building Block 6

Need for flexible and adaptive finance rules

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- ✓ Categorisation of IT expenditure as capex instead of opex.
- ✓ Budget constraints (including around multi-year commitments).
- ✓ Wasted spending.

Governments are spending more on IT, both in absolute terms and as a percentage of total government spending. Historically, funding of new IT capability has been treated as investment (CAPEX) with little scope to treat it as operating expenditure where costs accrue over time. Government departments are often required to apply for lump sum funding on an annual basis. This can inhibit longer-term strategic and foundational technology investments, including for cloud and digital transformation projects and drives a tendency for shorter term projects with more limited capability and return.

Budgets should in our view be reconsidered in the context of digital expansion to:

- enable a longer-term investment plan for IT and digital investment using multi-year budgets that facilitate multi-year commitments to consumption.
- adopt a flexible model to allow more rapid deployment of budget, avoid inefficient spending decisions and wasted budget. For example, implementing spending limits to allow users to have instant access to the services they need, while larger projects with higher spending have more governance and oversight;
- ensure that government budgets encompass not only IT services, but also support services, investment in guidance and training (see Building Block 7 (The importance of a collaborative approach between different parts of government, and between government, regulators and/or the private sector), and Building Block 8 (Promotion of a digital culture and civil servant upskilling)).

We believe that it is advantageous for governments to have a clear financial plan that sets out technology spending priorities and ensures spending outside of those priorities is avoided. IT expense needs to be targeted, controlled and optimised. A lack of planning may lead to payment issues, or the need to request additional services that fall outside an annual budget. Financial guides/instructions could be issued to allow departments to estimate their consumption more accurately or modify it.

In addition to budget allocation and funding considerations, accountability and transparency around use of funds is important. Ministries are not always able to identify resource allocation because it is distributed across multiple accounting items or is poorly visible in the budgets of other non-IT programs. Instead, a uniform methodology should be adopted to allow consistent reporting of expenditure and mechanisms should be introduced to track and evaluate cloud spending (and any potential savings made). This can track not only spending across projects, but also tracking projects against their bae business case over time.

In the next spread, we set out a few examples from the UK[75,76], Australia[77], Singapore[78], Argentina[79] and Finland[80].

United Kingdom (Spend Controls and Red lines for IT procurement)

Spend Controls

Spend controls must be complied with by central government and are intended to help organisations reduce unnecessary spend and encourage cross-government collaboration. There is a particular approval and oversight process for digital and technology activities.

Red lines for IT procurement

In 2014, the UK government published 'red lines' for IT contracts which apply to all of central government. This was to encourage competition while delivering value for money for the taxpayer.

These are:

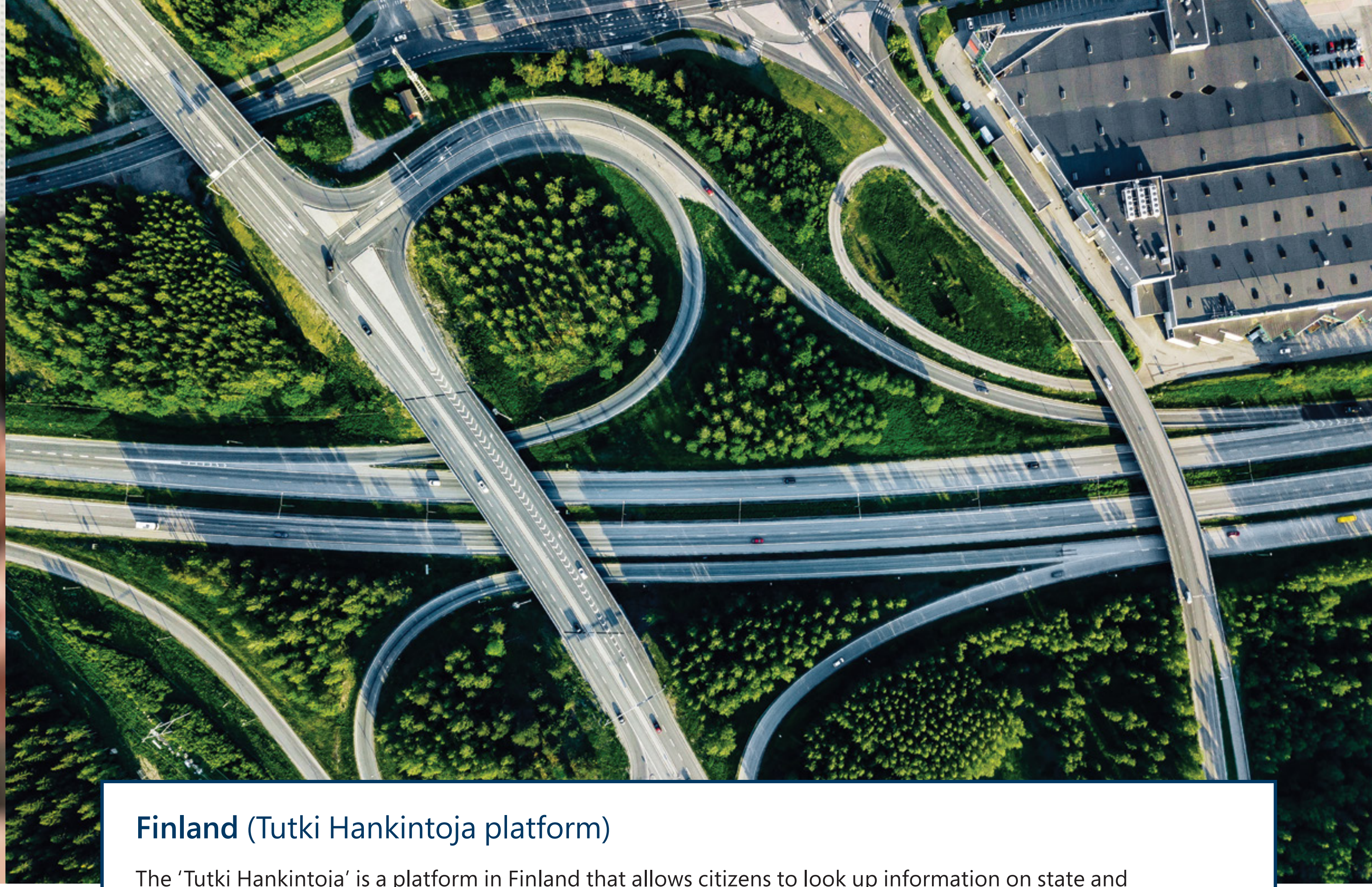
- no IT contract will be allowed over £100 million in value – unless there is an exceptional reason to do so;
- companies with a contract for service provision will not be allowed to provide system integration in the same part of government;
- there will be no automatic contract extensions; and
- new hosting contracts will not last for more than 2 years.

If a department breaches these redlines, their project will be subject to increased scrutiny.

Australia (Funding for cloud)

Australia's Digital Transformation Agency has noted that cloud as an on-demand service is an operational expense. Therefore, traditional budget cycles and classification of hardware and software as capital expenses may not suit agile ways of working and the deployment of cloud services.

Given the Australian government's cloud-first policy (as detailed above), the DTA has expressly provided for a process for converting capital expenditure allocation to operational expenditure, so that these can be applied towards larger cloud projects.



Finland (Tutki Hankintoja platform)

The 'Tutki Hankintoja' is a platform in Finland that allows citizens to look up information on state and municipal procurement. It is searchable by citizens and businesses and allows them to view what and how the government has spent on procurement projects. This provides access to how public funds are spends and also breaks down information on IT procurement by state and municipal level.

The website also tracks total spending year-to-date and the number of suppliers and paid invoices made by the Finnish government.

Argentina (Business case certification)

In Argentina, the National Office of Information Technologies (ONTI, Oficina Nacional de Tecnologías de Información) leads the process on how ICT projects are planned and approved at the central level. ONTI has published technical standard and technical requirements for ICT projects.

In addition, ONTI reviews ICT project proposals with its guidelines and where satisfied, it provides non-binding certification when business cases of such project proposals are reviewed and approved by ONTI.

Singapore (government commercial cloud)

The Singapore government launched the Government on Commercial Cloud project in 2019 to homogenise the onboarding experience and administrative tasks of government agencies on the cloud. Framing cloud offerings as an 'infrastructure' project accelerates the procurement process by granting government agencies quick clearances for cloud service procurement from private sector offerings.

Building Block 7

The importance of a collaborative approach between different parts of government, and between government, regulators and/or the private sector

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- Disconnect between regulation and digital transformation objectives.
- Lack of a clear understanding of issues and priorities faced by different stakeholders. Stakeholder issues/priorities are often viewed in isolation. The expertise and value of different stakeholders/perspectives is often overlooked.
- Absence of a holistic digital roadmap.
- Technology providers seen as vendor of goods/services only, and their expertise and experience in digital transformations may not be utilised to the full advantage of a government seeking digital transformation.
- Technology providers often have not earnt the trust of governments.

Although most governments recognise the value of technology, in our experience, a lack of collaboration and/or a disconnect in digital strategies and priorities between different parts of government (including policy makers, procurement, budget departments and IT) and a lack of collaboration between government, regulators and/or the private sector can hinder the success of a country's digital transformation journey.

Internal Government Alignment

Governments that understand the true potential of technology and have had success in realizing their digital transformation objectives, have incorporated the goal of digital transformation into management policies and strategies. Importantly, they have utilized the breadth of expertise and perspectives by adopting a collaborative approach across stakeholders, ensuring each constituency is "bought in" to the journey and committed to its implementation and success.

However, in practice, despite the obvious benefits of this collaboration, it is not always readily achieved. There are diverse reasons for this in our view, but one key cause is that there are often different levels of appreciation of the cloud and other digital technologies between stakeholders. Whilst IT teams and specialist procurement functions often have a solid understanding of digital technologies, the same may not be true of other areas of government, including at times those that set policy that affects IT procurement. This difference in appreciation can lead to frustration and debate over digital transformation initiatives, causing timetables to slip or entire transformation projects to be abandoned entirely. We understand realizing a collaborative approach is a journey in itself, and training of stakeholders on the technology (see Building Block 8 (Promotion of a digital culture and civil servant upskilling)) is just as important as engaging stakeholders on the objectives of the digital transformation journey.

Given the fast pace of innovation, it is also essential to continue this collaborative and educative approach throughout the lifecycle of technology implementation as it will help inform the success of a country's digital roadmap in areas as broad as legislative change, transparent communication, governance and oversight, procurement of services, evaluation of success, and future innovations.

Leveraging All Stakeholders

Collaboration is not only necessary between government stakeholders, but also advantageous when undertaken between government, regulators and the private sector. Technology suppliers are sometimes seen only as vendors of goods and services. Clearly, they are vendors, but they also have deep subject matter expertise of public sector digital transformation and innovation more generally (see the Nigerian example below) which should be harnessed. Careful use of this resource can give governments access to experience drawn from a deeper pool of expertise than governments alone can draw on. Where it is done with care, using digital providers' expertise should not compromise the commercial leverage that a good procurement strategy should deliver (see Building Block 4 (A centralized procurement function / central purchasing entity). There will be times, for example during major procurement processes when the risk of compromising procurement rules may outweigh the benefits to be gained, but outside these periods, most mature providers will in our view welcome such dialogue and collaboration. Under its major contracts, governments should expect such discussions on a regular basis as part of their service scope, during contract term. It is worth noting that there are also actions that technology providers need to take to earn the trust of governments, to encourage such dialogue, including during the procurement process, being clear what is being committing to, being able to explain those commitments clearly and ultimately meeting those commitments.

Inter-Governmental Engagement

In the spirit of supporting the advancement of the global public sector digital transformation journey, collaboration between countries in respect of their digital priorities and challenges is also useful. The UK Government Digital Services frequently hosts agencies from around the world and emphasises the value of exchanging insights and experiences between countries.[81]

As follows, we have included various examples of collaboration utilised by the Singaporean[82,83], UK[84], Danish[85,86,87], and Nigerian[88,89] governments in their digital transformation.

United Kingdom (One Government Cloud Strategy)

The UK recognises the importance of government organisations and functions working together to take advantage of the benefits of cloud technology.

It has a 'one government cloud strategy' for government workers responsible for cloud strategy and implementation, which covers how to enable cross-functional collaboration throughout the cloud lifecycle, realise best practice cloud service usage and maximise commercial, technical, security and people capabilities.

The successful implementation of this policy culminated in the Home Office reducing its cloud portfolio spend by 40% as a result of a joint technical and commercial approach to cost optimisation.

Singapore (Smart Nation Strategy)

The Singapore government outlined its commitment to digital transformation in its Smart Nation strategy. It set up a Smart Nation and Digital Government Office in 2017.

The Singapore government has stated on its website that as of 2022, 95% of all transactions with the Singapore government are digital from end-to-end. The goal is for almost 100% of transactions to be carried out digitally by 2023. The government has set out specific goals to achieve its digitization objective. The ambition is to leverage data and harness new technology to enable the government to improve its quality of service delivery, increase efficiency and productivity, and enable new and better means of engaging with people and business.

Underpinning its success are several factors including political commitment of the authorities, robust leadership and institutionalization, coordination between government agencies, as well as solid financial support.

Denmark (Digital Ready Legislation – Collaboration between legislators and civil servants)

Since 2018 it has been mandatory to assess whether new legislation is "digital-ready". This means ensuring the legislation complies with seven digitization principles, which include support of digital communications, safe and secure data handling, and digital administration of the legislation. Historic legislation is also being reviewed.

This relies on a collaborative approach between legislators and civil servants. A public impact assessment is also undertaken by the relevant ministry.

An example of this is the introduction of legislation defining responsibility for violation of vehicle access restrictions in urban areas. It enables the automatic administration through licence plate scanners and a central vehicle register as an alternative to manual enforcement.

Nigeria (Collaboration with Microsoft)

The Nigerian government is collaborating with Microsoft to accelerate its digital transformation.

In a recently published Microsoft position paper, Microsoft presented recommendations to drive cloud adoption and catalyse digital transformation, including amplification of government communications showing its commitment to ICT policies (including cloud first) and implementation of Nigeria's data interoperability framework across the public sector.

Building Block 8

Promotion of a digital culture and civil servant upskilling

Implementation of this building block will assist countries to overcome the following challenges to a successful digital transformation:

- ✓ Limited understanding of digital transformation and its benefits.
- ✓ Lack of articulation of clear digital goals.
- ✓ Skill gaps.
- ✓ Mistrust of digital.

One of the key components of digital transformation is people. Governments need stakeholder buy-in and a willingness to adopt a digital way of working. In addition, having digital talent and skills is fundamental for an effective and sustainable digital transformation strategy and journey.[90]

Executive buy-in

Strategic leadership and executive influence are crucial. In addition, having a team dedicated to IT investment guidance and cloud deployment decisions is one of the most effective ways to achieve rapid results and influence the process of change. In both cases, it is important that both have a good understanding of cloud and other digital technologies to ensure they are able to properly assess the merits of digital transformation.

Governments should consider a Cloud or Digital Transformation Center of Excellence (CoE). This would be a team of people dedicated to the creation, spread and institutionalisation of best practices, structures and governance for the evolution of cloud and digital transformation technology. Some of the functions of a CoE include promoting cross government collaboration, identifying training needs, provide customised training and influence cultural change.

Upskilling of civil servants

An understanding of the cloud and other digital technologies is not only important for the use of such technologies, but is also necessary to ensure stakeholders across government can collaborate on the policies and strategies associated with a government's digital transformation. (See also Building Block 7 (The importance of a collaborative approach between different parts of government, and between government, regulators and/or the private sector)).

Governments should consider performing an analysis of skill gaps, including a review of the current state of the government IT workforce and projection of future skill requirements. As with many new technology initiatives, governments must expect employees to be trained en masse in the use of cloud technologies. Training should not be constrained to technical, but also to contracting and procurement (i.e., procurement team having the knowledge to keep up with the growing list of technology solutions).

A workplace training program should enable the government to attract, train, and support workers with the skills needed for the next stage of digital growth.

In an OECD Government at a Glance report, 76% of OECD countries surveyed have strategies for the development of both user skills (e.g. email management) and professional digital skills (i.e. initiatives to attract and maintain specialists in digital technologies in the public sector) among civil servants.[91] However, only 41% have conversion processes to increase the number of ICT professionals, only 62% focus on digital complementary skills (i.e. increasing awareness of the opportunities, benefits and challenges of the digital transformation of the public sector).[92]

Maintaining digital competence is an ongoing process – there needs to be a constant dialogue within an organisation between the strategic, product development or technical functions with the human resources function to ascertain the specific skills required that need to be developed. Once these are determined, the strategies deployed for upskilling can be through 'building' the skills through upskilling and training, 'buying' skills through recruitment of new staff, or 'borrowing' the skills by engaging contractors or arranging fellowship arrangements.[93]

Shift in workplace culture

A shift in workplace culture may also be required as often there is a resistance to change. Employee communication, engagement, and transition strategies are key. Governments must implement communication plans that help employees understand the changes that need to be made to implement technology. For example, cloud migration may require deactivation of systems that have been in use for many years. Employees may be reluctant to learn how to operate new systems in a cloud environment, especially if jobs are redefined. It is imperative to build an understanding of digital transformation benefits and how cloud-based technologies work.

A few examples of how governments around the world (the UK[94,95], Canada[96], Philippines[97] and Singapore[98]) have implemented this building block are set out, as follows:

United Kingdom (Office for National Statistics Shift in Workplace Culture)

The UK Office for National Statistics wanted to move some of its services to the cloud. Senior leaders were concerned that putting data in the cloud would cause security issues. There were also people in the organisation who did not want to change and work in a new way.

The training budget was increased to invest in upskilling staff for the movement to the cloud. In addition, various methods were employed to get staff comfortable with the shift. Round table discussions with experts and other workshops were held to allow staff to find out more about cloud usage.

In terms of lessons learned, the ONS has noted that one thing it would do differently would be to have more staff engagement from day 1 of the project. Being open and honest about the cloud strategy and cultural change was seen as very important.

Singapore (The Digital Academy)

GovTech Singapore established The Digital Academy as a technology focused learning institute for the public service. This learning platform was developed in partnership with industry players including Microsoft and covers areas like data science, apps development, product management, amongst others.

United Kingdom (GDS Academy)

In the UK the 'GDS Academy' trains public sector workers in how to work in an agile team and how to design a digital service.

Canada (Digital Academy)

A Digital Academy was established by the Canada School of Public Service in 2018. This helps federal public servants to gain the knowledge, skills and mindsets they need in the digital age.

Philippines (ICT Literacy and Competency Development Bureau)

The Philippines' Department of Information and Communications Technology implemented an Assess-Build-Certify (ABC) Framework through its ICT Literacy Competency and Development Bureau. The aim of this framework is to develop competencies and training needs for individuals in different ICT areas, and programmes offered include webinars as well as courses on digital governance and management and digital transformation.

D

A Snapshot of Digital Transformation Journeys

"Building" on the building blocks in Section C above, this section showcases the digital transformation journeys of the United Kingdom, Singapore and Australia.

United Kingdom

The United Kingdom has one of the most digitally advanced governments in the world. In the 2019 OECD Digital Government Index, the UK was ranked 2 overall and ranked 1 for having a data-driven public sector, due to the government's use of cloud-based solutions to encourage inter-departmental data flows, in part stemming from its 'one government cloud strategy' (see Building Block 1 (Adoption and implementation of a National Cloud Strategy and Cloud First Policy)).[99]

Early days of UK government digitalization

The UK government's digital transformation began in 2011, with the establishment of the Government Digital Service (GDS) (a newly created arm of the UK government's Cabinet Office), which set out to transform the public sector by implementing user-focused digital services through the 'Digital by Default' strategy (DbD Strategy). This strategy estimated that moving services from offline to digital channels would save between £1.7 and £1.8 billion per annum.[100]

The DbD Strategy sought to create a consistent inter-departmental approach to digital services. It set out a number of key principles, including improvement of departmental digital leadership, developing digital capability throughout the civil service, removing unnecessary legislative barriers and improving the way that government makes policy and communicates with people.[101]

The UK government has released various policies and strategies since then to embrace the move to digital and emerging technologies. All have focused on using digital transformation to:

- enhance cross-government collaboration;[102]
- adopt more cost-effective IT solutions;[103] and
- create a public sector which transforms and designs its services around the needs of users (including citizens).[104]

Digitalization in practice

Public sector agencies are able to purchase a variety of digital services through the Digital Marketplace by using one of the Crown Commercial Services (CCS) three frameworks:[105] (1) G-Cloud; (2) Digital Outcomes and Specialists; and (3) Crown Hosting Data Centres. See also Building Block 5 (Use of whole of government framework agreements):

- **G-Cloud:** From 2013 to 2020, the government's cloud first policy (see Building Block 1 (Adoption and implementation of a National Cloud Strategy and Cloud First Policy)), led to significant expenditure on G-Cloud, with the public sector purchasing cloud technology such as hosting, software and support and managed services, including many off-the-shelf, pay-as-you-go cloud solutions. The G-Cloud framework allows for flexible use of cloud computing.[106] Different government agencies are able to share cloud solutions, moving away from traditional, expensive IT services to cheaper cloud technologies which are accessible, scalable and easily maintainable.[107] For example, in response to the COVID-19 pandemic, the Department of Health and Social Care used G-Cloud to purchase hosting services for the NHS Test and Trace programme known as 'Halo'[108,109].
- **Digital Outcomes:** The Digital Outcomes framework enables government agencies to develop and research digital solutions before implementing a live version of the relevant services.[110] The COVID-19 pandemic again demonstrated the significant value of this framework, as it ensured a beta phase of the NHS vaccine booking system could be tested and refined, ultimately leading to an efficient, targeted roll-out of the service.[111]
- **Crown Hosting Data Centres:** The CCS recently published a new version of the Crown Hosting Data Centres framework called 'Crown Hosting II', which will run on a seven-year contract from March 2023 at an estimated value of £250 million once signed[112]. The proposed data centre services will store data critical to national interest or with higher security classifications and will therefore maintain high physical, operational and electronic security.[113] This reflects the government's prioritisation of cybersecurity, but also points to its cloud first policy by encouraging government bodies to migrate large volumes of less critical data to the cloud.[114]

Use of data

The 2020 National Data Strategy (NDS) demonstrated the government's vision to build a world-leading data economy.[115] The NDS aims to ensure that businesses and citizens trust the UK's data ecosystem, are sufficiently skilled to operate effectively within it, and can access data when they need it.[116] The NDS also provides coherence and impetus to the broad array of data-led work across government, while creating a common understanding of how data is used.[117] In addition, the NDS Forum seeks to refine the implementation of the NDS and how the government can support the responsible and trusted use of data in the UK.[118] The forum is a structured programme of engagement which brings together a diverse range of perspectives from industry, academia and the public sector to: (1) increase collaboration to support the delivery of the NDS; (2) champion the NDS through wider networks, to embed its principles and goals beyond government; and (3) help shape the future vision of the NDS.[119] Although the forum has no decision-making power, it has identified five themes, now central to the government's implementation of the NDS, which are:

- unlocking the power of data for everyone everywhere (make data more useable, accessible and available);
- trust in data;
- data reform (creation of an innovation-friendly data protection regime which supports peoples' trust in data);
- net zero (harness the power of data to meet net zero ambitions); and
- measuring the data ecosystem (mapping stakeholder activity across the data ecosystem).[120]

In addition, in September 2021, as part of the NDS, the UK Government launched its consultation; 'Data: a new direction' to inform proposals to reform data protection laws and secure a pro-growth and trusted data regime. Running for ten weeks and receiving 2,924 responses, several key themes emerged from the process including that;

- Respondents value the importance of maintaining data subject rights, with the intention of building on the current UK GDPR regime.
- Respondents made clear that they see benefits from the effective use of personal data that the proposed reforms would deliver – however this must be done responsibly.

- Respondents raised the importance of data flows with the EU, and how our reforms will affect this (particularly with the UK's EU data adequacy decision.)

Overall, responses indicated support for the government's proposals in many areas, including:

- changes to research provisions, especially the proposal to consolidate and bring together research-specific provisions, to create a statutory definition of 'scientific research' and the changes proposed to notification requirements;
- removal of consent requirements in relation to audience measurement cookies;
- the principle of proportionality outlined in the reform agenda across adequacy and Alternative Transfer Mechanisms (ATMs);
- reforming the ICO, and emphasis on the importance of maintaining its regulatory independence;
- standardising the terminology and definitions used across the data processing regimes;
- increasing clarity and transparency of the existing rules on police collection, use and retention of data for biometrics, in order to improve transparency and public safety; and
- extending powers under section 35 of the Digital Economy Act 2017, to include businesses, as this could be beneficial in terms of joined-up public services.

However, there were some potential concerns raised about:

- introducing a nominal fee for subject access requests;
- whether the government should have a role enabling the activity of responsible data intermediaries;
- removing the need for data controllers to carry out the legitimate interests balancing test for specified activities if children's data were involved;
- removing the right to human review of automated decisions;
- whether to exclude political parties and charities from rules on direct electronic marketing;
- removing requirements for Data Protection Impact Assessments (DPIAs) and Data Protection Officers (DPOs); and
- the potential impact of reforms on the ICO's independence.

Regulatory challenges

The transition to digital (including cloud computing) created a new set of regulatory and cybersecurity challenges.[121]

In July 2021, the Department for Digital, Culture, Media and Sport (DCMS) published a policy paper: 'Digital Regulation: Driving Growth and Unlocking Innovation' (Plan for Digital Regulation).[122] The paper highlighted the government's safe and responsible development of public service technologies (shown by the government's balanced use of data centre or cloud services relative to data criticality as discussed above), whilst ensuring cloud service providers and data driven / artificial intelligence technologies are appropriately regulated.[123] This paper demonstrates the UK government's willingness to shape regulation which balances the need for citizen trust with the value of innovation, a particularly important element for the proposed roll-out of digital identity solutions, due to security and privacy concerns over the processing of sensitive personal data.[124]

Due to this responsible approach, the UK government is both a global frontrunner when it comes to innovative digital technologies and a leader in developing digital regulations that set the global standard.[125] For example, the government established the Digital Markets Unit in 2021 which facilitates competition across digital markets, thereby sustaining opportunities for smaller technology providers and supporting innovative products available at competitive prices.[126] The government has also empowered Ofcom to regulate video sharing platforms and, under the proposed Online Safety Bill, enshrine in law a duty of care on online companies to keep users safe.[127]

Brexit

As part of the Plan for Digital Regulation, the government also sought to reduce the potentially negative impacts of Brexit by encouraging the use of innovative digital solutions to streamline administrative burdens on businesses.[128] For example, in respect of filing complex trade documentation.[129] This has helped to keep costs down and maintain continuity of supply during the uncertain period of European trade between the UK and the EU.[130]

Cultural shift to digital

Aside from regulatory issues and cybersecurity concerns, the UK government overcame a great deal of resistance to change by upending deeply entrenched public sector methods.[131] For example, before 2010 each government department had a separate website, and as part of the DbD Strategy, GOV.UK was created, with more than 2,000 websites migrated to the new single publishing platform.[132]

It also recognised the importance of having a digital culture and skill set across government departments. For example, the Office for National Statistics increased investment in training on the use of cloud services (see Building Block 8 (Promotion of a digital culture and civil servant upskilling)).[133] The GDS also runs an academy with courses aimed at civil servants and other public sector workers to upskill public bodies through training and development.[134] The NHS Digital Learning & Development team recently partnered with the GDS to create an inter-departmental relationship for training NDS employees on various digital services.[135]'

By partnering with the GDS, as opposed to a non-governmental or private training provider, the NHS saved considerable sums on its training and development budget.[136]

The government's wider focus on skilled jobs creation through digitization both inside and outside the public sector has paid off. Data published by the DCMS shows that the digital sector added up to £150.6 billion to the UK economy in 2019, supporting 1.56 million jobs.[137] Additional research from the DCMS shows that if the government continues to support the digital sector, a further 678,000 jobs could be created by 2025 across the country.[138]

Further capitalizing on existing momentum towards an all-up public sector digital revolution, efforts to strengthen the UK's position as a Global Science and Tech Superpower continues to accelerate. In a June 2022 announcement of a new Digital Strategy, the Minister for Tech and the Digital Economy expressed a desire to "go further and to go faster", with the goal to set the UK apart as the best place to start and grow a technology business. The Strategy lays out this vision in detail and the actions required to deliver against it. Bringing together existing and new programs in a cross-cutting digital policy agenda, the Strategy covers almost every aspect of the government's reach across the digital economy. While it reiterates already published initiatives, it also highlights flagship new policies. For example, it lays out a strategy for government-led review of the UK's most advanced computing capabilities with the aim of understanding the UK's compute needs over the next decade and its role in delivering on the ambition to strengthen its position as a global tech leader. The Strategy focuses on six key areas which are defined as: 1) digital foundations, 2) ideas and intellectual property, 3) digital skills, 4) financing digital growth, 6) spreading prosperity and levelling up, and 6) enhancing the UK's place in the world.

Looking ahead

In May 2021, the GDS published its strategy for 2021-2024.[139] This highlights the government's continued focus on the joining up of services and the sharing of data across departments.[140] This approach aligns with the Home Office Digital Data and Technology's (DDaT) strategy to converge technologies through the uptake of cloud services, creating inter-operable technology products which further foster cross-government collaboration.[141]

The government's aim to transition away from traditional forms of identification such as passports and driver's licences to digital identities, demonstrates its vision to benefit from opportunities that the wider digital economy offers.[142] (See also Building Block 3 (Adoption and implementation of a digital identity strategy)).

The UK government's digital journey is a continuing and evolving one. Reflecting on the COVID-19 pandemic, it is clear that the government's focus on digital transformation enabled it to manage the crisis through the likes of the Halo platform.[143] Going forward, much of the government's thinking about how to 'build back better' post-pandemic relies on digital innovation.[144] The government is currently committed to delivering several ambitious and interlinked policies to prepare the UK for an increasingly digital world. The National Data Strategy will soon be complemented by a new wave of strategies, including the Innovation Strategy, AI Strategy, Digital Strategy and National Cyber Strategy.[145] Such initiatives, alongside enabling legislation, will facilitate the government's Ten Tech Priorities, which set out its ambitions to build 'a world-class digital technology sector, keep the UK safe and secure online, and fuel a new era of start-ups and scaleups'.[146]

Singapore

The Singapore government's digital transformation journey had its early beginnings in the 1980s when the National Computer Board was set up to computerise the civil service.[147] The national digital identity (SingPass) was launched in 2003 to provide Singapore residents with access to government digital services, and with increasing connectivity and widespread use of technology, the government outlined its plans to turn Singapore into a Smart Nation in 2014.

Today, the Smart Nation roadmap brings together three prongs: digital government, digital economy and digital society. To develop a 'digital government', the Digital Government Blueprint was developed to measures 14 key performance indicators to measure how the Singapore government's digitalization journey progressed.[148] Several goals were outlined as part of this strategy, including the following:

- migrating at least 70% of eligible government systems to the commercial cloud by 2023;
- training all public officers to have basic digital literacy skills;
- completing at least 10 cross-agency high impact data analytics projects every year; and
- having no more than 7 working days to share data for cross-agency projects.

In addition, the government is seeking to foster the growth of a 'digital economy' and 'digital society' so that businesses and individuals are also adopting technology at a rapid pace and benefiting from the digital ecosystem.[149]

This commitment to digitization was cemented by the establishment of the Government Technology Agency of Singapore (GovTech) in 2016, which focused on beefing up the government's own technical capability so that the government can develop and deliver digital products and services for its citizens.[150] GovTech is the centralized agency developing these digital products for the whole of government. This framework also makes it easier for digitalization projects to be rolled out across the government rather than in a piecemeal fashion.

A sample of the digital products and services available include the following:

- Parking.sg: a mobile application that allows users to pay for short-term parking charges through their mobile devices at all public car parks (replacing paper parking coupons);[151]
- LifeSG: a suite of services which consolidates digital solutions based on specific moments in citizen's life journey. For example, on having a child, citizens can use the app to register the child's birth, apply for various grants and subsidies, and access immunisation records;[152] and
- GoBusiness: a platform which connects business owners to various government e-services and resources so they can register a business, apply for licences and grants with personalised recommendations.[153]

When the COVID-19 pandemic arrived on Singapore's shores, the government was one of the fastest in the world to respond by setting up a suite of digital products to contain the outbreak. For example, the TraceTogether app was developed to enable contact tracing and enabling individuals to keep track of whether they may have been in close contact with infected individuals.[154] This ability to respond swiftly is underpinned by having a robust digital infrastructure and an ongoing commitment to develop technical capabilities in-house within the government.

In addition to providing digital 'government' products and services for residents, the Singapore government has been actively collaborating with the private sector – one key initiative arising from such collaboration is the creation of data exchanges, which is a form of public digital infrastructure:

- in December 2020, the government launched the Singapore Financial Data Exchange (SGFinDex) in collaboration with seven participating banks – this allows an individual to consolidate their financial data from various banks and the government, such as account balances, credit cards, investments, housing, pension, taxes, and view this data on a single platform;[155] and
- the government also recently launched the Singapore Trade Data Exchange (SGTraDex) on 1 June 2022 which is a collaboration between the Infocomm Media Development Authority of Singapore with certain supply chain players such as banks, port operators, commodity traders and energy companies to create a trusted 'digital infrastructure' to manage data sharing along the supply chain.[156]

Australia

The Australian government has adopted a range of digital innovation in recent years and has made strong progress in digital transformation. The Digital Transformation Agency of the Australian government (DTA) was established to be the responsible agency for "strategic and policy leadership on Whole-of-Government and shared information and communications technology (ICT) investments and digital service delivery".[157] This consolidates government policy and sets the direction for ongoing public sector digital transformation.

The Digital Transformation Strategy was initially released in 2018 (and was last updated in 2021), and sets out a shift of focus to accelerate digital transformation within government for Australia to become one of the top three digital governments in the world by 2025.[158] The strategy includes the following ambitions for Australia's digital future[159,160,161]:

- the Digital Government Strategy – "accelerates digital transformation for Australia to become one of the top three digital governments in the world by 2025".
- the Digital Economy Strategy – which focuses on the "broader Australian Economy and the delivery of secure and trusted digital government services".
- the Australian Data Strategy – which sets out a clear vision for Australia's data capability.
- the Secure Cloud Strategy – which helps agencies to move to the cloud; and
- the Hosting Certification Framework – which provides policy direction and guidance applicable to the Australian government's facilities and infrastructure hosting ecosystem.

The Australian government has identified six strategic outcomes that are essential to achieving its outcomes and driving consistency in its delivery, including three strategic outcomes for the government as follows:[162]

- Architecture alignment – Platforms and services will be connected within the Whole-of-Government Architecture.
- Re-use and investment – We will build a culture of reuse backed by modern digital capabilities.
- Digital workforce – Our government will be fit for the digital age, empowered by digital skills, capabilities and tools.

Digital services delivered by Australian government include, for example:

- myGov, a secure way to access government services online in one place;[163]
- GovPass, a new digital identity solution to make it simple, safe and secure to prove the identity of users when they access government services online;[164]
- My Health Record, an electronic health record system which is accessible by healthcare providers and consumers and contains over 23.3 million individual records and 629,000,000 medical documents;[165,166] and
- Business Registration Service, a solution to combines a number of key government business and tax registration forms in one place, reducing the average time taken to register for an Australian business number from over an hour to less than 15 minutes.[167]

The Australian government is also exploring opportunities to use technologies such as artificial intelligence and blockchain to enhance government service delivery. For instance, in May 2016, the Australian government launched a virtual assistant, named Alex, to answer customer queries relating to IP rights and related information.[168] The government also launched an AI action plan in June 2021 which sets out a plan to build Australia's capability in artificial intelligence for economic growth and job creation, amongst other benefits.[169]

Recent publications and developments also include:

- A 'Blueprint for Critical Technologies' published in November 2021 contains a framework for how to capitalise on critical technologies, and sets out 'action pillars' such as upskilling Australians in critical technologies and ensuring policies, regulation and standards are fit-for-purpose.[170]
- As part of the National Quantum Strategy, the government set up a Quantum Commercialisation Hub to form strategic international partnerships by Australia and to commercialise Australia's quantum research. Quantum is one of the nine technologies for initial focus in the government's Blueprint for Critical Technologies.[171]

E Next Steps

In this paper, we have provided an overview of what we consider to be the essential components of a successful public sector digitization policy and procurement strategy.

We have intentionally kept our examination of each of each of the building blocks at an informative altitude, and we understand that successful operationalization of each pillar, will require an in-depth examination of each country's specific social, economic and geo-political context as well as an exploration of the interrelationships between the various laws and regulations that may be implicated by each building block.

We also believe that the journey to digital transformation is a constantly evolving one, punctuated by pivots and altered by individual national responses to an ever-changing global policy climate.

Microsoft's Worldwide Public Sector Global Market Development (GMD) Team Engagement.

It is our aim to follow-up this paper with a series of workshops with our public sector community of customers, during which we will engage in deeper discussions on each of the building blocks. We also plan to publish a series of more detailed papers, each focused on a single building block and the specific factors that underpin successful implementation.

As a team, GMD is primed to provide these sorts of insights. GMD is by design an incredibly diverse group, made up of former senior civil servants, technologists, regulatory and policy experts, development professionals, and technology consultants. A team diverse in experience and geographical spread; whose knowledge we activate as we engage with the public sector community to help empower it to maximize opportunities for cloud and digital transformation technologies, co-creating demand for technology that will benefit all market ecosystem players so that all participants; government, citizens, and the community benefit in a true "win-win-win" situation. At Microsoft, our commitment to ensuring that our product and service offerings respond to the explicit needs of our public sector clients, informed by our focused and concerted partnership with public sector elites across the globe, has created a powerful incentive to adopt an informed and strategic approach to policy engagement.

We have demonstrated this commitment to targeted engagement through the delivery of on-demand policy assets and expert analyses that are currently leveraged by our public sector partners across the globe. Through our Public Sector Center of Expertise, we curate this research and thought leadership and highlight the impact of public servants who are leading the charge towards digital transformation and innovation in the public sector.

The serial exploration of the policy and procurement building blocks through workshops and publications that will follow this paper will further expand this body of knowledge and ensure that we make good on our commitment to continually share our voice and perspective on the future of successful digitization across the globe.

F References

General reference

The following reference has been used generally throughout this paper: Antonio García Zaballos, Enrique Iglesias Rodríguez, Pau Puig Gabarró and Tomás Campero, 'Public procurement of cloud computing services: best practices for implementation in Latin America and the Caribbean' (Inter-American Development Bank, sponsored by Microsoft, 2020) (the "IADB-Microsoft Public Procurement Paper 2020").

Specific References

1 OECD Directorate for Public Governance, 'Government at a Glance 2021' (OECD, July 9 2021), Chapter 10 'Digital Government', <https://www.oecd-ilibrary.org/sites/1c258f55-en/1/3/10/index.html?itemId=/content/publication/1c258f55-en&_csp_=10e9de108c3f715b68f26e07d-4821567&itemIGO=oecd&itemContentType=book> accessed June 2022

2 Deloitte Insights, 'Seven pivots for government's digital transformation, How COVID-19 proved the importance of "being" digital' (Deloitte Center for Government Insights, 3 May 2021) <https://www2.deloitte.com/content/dam/insights/articles/6974_CGI-Digital-2/DI_CGI-Digital-2.0.pdf> accessed June 2022. Pursuant to a government survey undertaken by Deloitte, three-fourths of respondents indicated that Covid-19 had accelerated their government's digital transformation, yet 80% of respondents did not think their digital efforts had not gone far enough.

3 Deloitte Insights, 'Seven pivots for government's digital transformation, How COVID-19 proved the importance of "being" digital' (Deloitte Center for Government Insights, 3 May 2021) <https://www2.deloitte.com/content/dam/insights/articles/6974_CGI-Digital-2/DI_CGI-Digital-2.0.pdf> accessed June 2022

4 IADB-Microsoft Public Procurement Paper 2020 (p.11). The Paper quotes several studies that report the positive impact on the economy resulting from the digital transformation of governments: Accenture (2013); OECD (2019); UNDESA (2011 to 2019). The impact of cloud-based technologies can also be consulted at the European Commission (2016).

5 IADB-Microsoft Public Procurement Paper 2020, p.18

6 IADB-Microsoft Public Procurement Paper 2020, p.19

7 Nigeria National Information Technology Development Agency, 'Nigeria Cloud Computing Policy' (Government of Nigeria, August 2019) <https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf> accessed June 2022

8 GovTech Singapore, 'Doubling down on cloud to deliver better government services' (Government of Singapore, 24 June 2020), <https://www.tech.gov.sg/media/technews/doubling-down-on-cloud-to-deliver-better-government-services> accessed June 2022

9 Department of Finance, 'Australian Government Cloud Computing Policy - Smarter ICT Investment' (Australian Government, October 2014) <https://www.ospi.es/export/sites/ospi/documents/documentos/Australian-Government-cloud-computing-policy.pdf> accessed June 2022

10 Digital Transformation Agency, 'Secure Cloud Strategy' (Australian Government, October 2021) <https://www.dta.gov.au/our-projects/secure-cloud-strategy> accessed June 2022

11 Central Digital and Data Office, 'Government Cloud First Policy' (UK Government, 3 February 2017), <https://www.gov.uk/guidance/government-cloud-first-policy> accessed June 2022

12 Government Digital Service, 'Case Study: How the Home Office's Immigration Technology Department Reduced its Cloud Costs by 40%' (UK Government, 17 December 2019) <https://www.gov.uk/government/case-studies/how-the-home-offices-immigration-technology-department-reduced-its-cloud-costs-by-40> accessed June 2022

13 Government Digital Service, 'Case Study: How the FSA Moved Everything to the Cloud' (UK Government, 17 March 2021) <https://www.gov.uk/government/case-studies/how-the-fsa-moved-everything-to-the-cloud> accessed June 2022

14 Government Digital Service, 'Case Study How the Welsh Government Migrated Their Technology to the Cloud' (UK Government, 27 March 2020) <https://www.gov.uk/government/case-studies/how-the-welsh-government-migrated-their-technology-to-the-cloud> accessed June 2022

15 Government of Canada, 'Government of Canada Cloud Adoption Strategy: 2018 update' (28 July 2020) <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html> accessed June 2022

16 Microsoft News Centre Canada, 'Quebec government leading with its cloud first strategy' (19 October 2018) <https://news.microsoft.com/en-ca/2018/10/19/quebec-government-leading-with-its-cloud-first-strategy/> accessed June 2022

17 IADB-Microsoft Public Procurement Paper 2020, p.19

18 US Department of the Interior, 'Cloud Smart Strategy' (United States Government) <https://www.doi.gov/cloud/strategy> accessed June 2022

19 FAS Office of Information Technology Category, 'IT Services: Cloud Empowerment at USAID: A 10-Year Success Story' (United States General Services Administration, United States Government, 3 October 2019) <https://gsablogs.gsa.gov/technology/2019/10/03/cloud-empowerment-at-usaid-a-10-year-success-story/> accessed June 2022

20 FAS Office of Information Technology Category, 'NOAA Forecast: Clear Skies for Cloud Migration' (United States General Services Administration, United States Government, 18 June 2019) <https://gsablogs.gsa.gov/technology/2019/06/18/noaa-forecast-clear-skies-for-cloud-migration/> accessed June 2022

21 National Oceanic and Atmospheric Administration, 'NOAA's Cloud and Data strategies to unleash emerging science and technology' (United States Department of Commerce, United States Government, 7 July 2020) <https://www.noaa.gov/media-release/noaa-s-cloud-and-data-strategies-to-unleash-emerging-science-and-technology accessed June 2022

[22] Cabinet Office, ‘Government Security Classifications’ (UK Government, May 2018) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf> accessed June 2022

[23] Cabinet Office, ‘Whitehall starts using simpler security classifications’ (UK Government, 2 April 2014) <https://www.gov.uk/government/news/whitehall-starts-using-simpler-security-classifications> accessed June 2022

[24] Cabinet Office, ‘Policy paper: Security policy framework’ (UK Government, 8 February 2022) <https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework> accessed June 2022

[25] IADB-Microsoft Public Procurement Paper 2020, p.23

[26] National Institute of Standards and Technology, ‘Information Technology Laboratory CSRC: Glossary—“impact level”’ (United States Government, 2022) <https://csrc.nist.gov/glossary/term/impact_level> accessed June 2022

[27] National Institute of Standards and Technology, ‘Publications: SP 800-53B Control Baselines for Information Systems and Organizations’ (United States Government, 10 December 2020) <https://csrc.nist.gov/publications/detail/sp/800-53b/finalhttps://csrc.nist.gov/glossary/term/impact_level> accessed June 2022

[28] National Institute of Standards and Technology, ‘Publications: SP 800-53B Control Baselines for Information Systems and Organizations’ (United States Government, 10 December 2020) <https://csrc.nist.gov/publications/detail/sp/800-53b/finalhttps://csrc.nist.gov/glossary/term/impact_level> accessed June 2022

[29] Attorney-General’s Department, ‘Protective Security Policy Framework: Policy 8-- Sensitive and classified information’ (Australian Government, 28 September 2018) <https://www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information> accessed June 2022

[30] National Archives of Australia, ‘Implement fit-for-purpose information management processes, practices and systems’ (Australian Government, 20 May 2022) <https://www.naa.gov.au/information-management/information-management-policies/building-trust-public-record-policy/building-trust-public-record-managing-information-and-data-government-and-community/2-implement-fit-purpose-information-management-processes-practices-and-systems#action-11> and ‘Building interoperability’ <https://www.naa.gov.au/information-management/building-interoperability> and ‘Digital Continuity 2020 Policy’ (October 2015) <https://www.naa.gov.au/sites/default/files/2019-09/Digital-Continuity-2020-Policy.pdf> accessed June 2022

[31] IADB-Microsoft Public Procurement Paper 2020 p.24

[32] Olivia White, Anu Madgavkar, James Manyika, Deepa Mahajan, Jacques Bughin, Michael McCarthy, Owen Sperling, ‘Digital Identification: A key to inclusive growth’ (McKinsey Global Institute, April 2019) (the “McKinsey Report”) <https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx> accessed June 2022

[33] PwC, ‘Digital identity: Your key to unlock the digital transformation’ (PriceWaterhouseCoopers AG, 2019) <https://www.pwc.ch/en/publications/2019/digital-identity-whitepaper-web.pdf> accessed June 2022

[34] PwC, ‘Digital identity: Your key to unlock the digital transformation’ (PriceWaterhouseCoopers AG, 2019) <https://www.pwc.ch/en/publications/2019/digital-identity-whitepaper-web.pdf> accessed June 2022

[35] McKinsey Report p.17

[36] McKinsey Report p.29

[37] SPID Public Digital Identity System, ‘FAQ- Frequently Asked Questions’ (AGID: Agency for Digital Italy, 2022) <https://www.spid.gov.it/en/frequently-asked-questions/> accessed June 2022

[38] GovTech Singapore, ‘Media Factsheet, Singpass – Singapore’s National Digital Identity’ (Government of Singapore, 2021) <https://www.smartnation.gov.sg/files/press-releases/2021/Media%20Factsheet%20on%20Singpass%20National%20Digital%20Identity.pdf> accessed June 2022

[39] Department for Digital, Culture, Media & Sport, ‘New legislation set to make digital identities more trustworthy and secure’ (UK Government, 10 March 2022) <https://www.gov.uk/government/news/new-legislation-set-to-make-digital-identities-more-trustworthy-and-secure> accessed June 2022

[40] PwC, ‘Estonia—the Digital Republic Secured by Blockchain’ (PriceWaterhouseCoopers AS, 2019) <https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf> accessed June 2022

[41] Canadian Bankers Association, ‘Canada’s Digital ID Future- A Federated Approach’ (Spring 2018) p.5 <https://cba.ca/Assets/CBA/Documents/Files/Article%20Category/PDF/paper-2018-embracing-digital-id-in-canada-en.pdf> accessed June 2022

[42] Kate Milberry and Christopher Parsons, ‘A National ID Card by Stealth? The BC Services Card’ (The British Columbia Civil Liberties Association for the Office of the Privacy Commissioner of Canada Contributions Program, September 2013) <https://bccla.org/wp-content/uploads/2013/09/BC-Services-Card.pdf> accessed June 2022

[43] Digital ID & Authentication Council of Canada, ‘DIACC— Identity in Action Case Study: BC Services Card’ (2018) <https://diacc.ca/wp-content/uploads/2019/03/DIACC-BC-Case-Study-v0.8.pdf> accessed June 2022

[44] Government of British Columbia, ‘BC Services Card App’ <https://www2.gov.bc.ca/gov/content/governments/government-id/bcservicescardapp> accessed June 2022. This source includes a video titled ‘BC Services Card Mobile App’, published by the BC Public Service on 7 July 2020. It is available at <https://youtu.be/nWC7H3LGlrE> and was accessed June 2022

[45] Government of British Columbia, ‘BC Services Card App: Available online services’ <https://www2.gov.bc.ca/gov/content/governments/government-id/bcservicescardapp/available-online-services> accessed June 2022

[46] Unique Identification Authority of India, ‘Welcome to Aadhaar Dashboard’ (Government of India) <https://uidai.gov.in/aadhaar_dashboard/> accessed June 2022

[47] The Indian Express, ‘Aadhaar helped Indian govt save $9 billion: Nandan Nilekani’ (13 October 2017) <https://indianexpress.com/article/world/aadhaar-helped-indian-govt-save-9-billion-nandan-nilekani-4888601/> accessed June 2022

[48] OECD, ‘Centralised and Decentralised Public Procurement’ (October 2000) <https://read.oecd-ilibrary.org/governance/centralised-and-decentralised-public-procurement_5kml60w5dxr1-en#page2> accessed June 2022

[49] UK Government, ‘Digital Marketplace’ <https://www.digitalmarketplace.service.gov.uk/> accessed June 2022

[50] Australian Government, ‘Buy ICT’ <https://www.buyict.gov.au/sp> accessed June 2022

[51] Public Services and Procurement Canada, ‘Government of Canada Tenders on Buyandsell.gc.ca’ (Government of Canada, 2022) <https://buyandsell.gc.ca/> accessed June 2022

[52] European Commission, ‘Public procurement—Study on administrative capacity in the EU: Italy Country Profile’ (4th revision of the European Commission’s Public Procurement Action Plan, 2020) <https://ec.europa.eu/regional_policy/sources/policy/how/improving-investment/public-procurement/study/country_profile/it.pdf> accessed June 2022

[53] OECD, ‘Mexico’s e-Procurement System: Redesigning CompraNet through Stakeholder Engagement’ (OECD Public Governance Reviews, 2018) <https://read.oecd-ilibrary.org/governance/mexico-s-e-procurement-system_9789264287426-en#> accessed June 2022

[54] OECD, ‘Fighting Bid Rigging in Brazil: A Review of Federal Public Procurement’ (2021) <https://www.oecd.org/daf/competition/Fighting-Bid-Rigging-in-Brazil-A-Review-of-Federal-Public-Procurement-2021.pdf> accessed June 2022

[55] Rwanda Ministry of Finance and Economic Planning and RPPA, ‘UMUCYO: e-Procurement System for Rwanda: What is UMUCYO?’ (2022) <https://www.umucyo.gov.rw/> accessed June 2022

[56] UK Government, ‘Digital Marketplace’ <https://www.digitalmarketplace.service.gov.uk/> accessed June 2022 and Government Digital Service ‘Guidance: Buying services on the Digital Marketplace’ (UK Government, 1 October 2019) <https://www.gov.uk/guidance/digital-marketplace-buyers-guide?_ga=2.198796079.1267801843.1655295633-712377853.1655295633> accessed June 2022

[57] Crown Commercial Service, ‘Guidance: Public procurement policy’ (UK Government, 8 January 2021) <https://www.gov.uk/guidance/public-sector-procurement-policy#procurement-policies-for-technology> (section “Procurement policies for technology”) accessed June 2022

[58] Crown Commercial Service, ‘Agreement: G-Cloud 12’ (UK Government, 28 September 2020) <https://www.crowncommercial.gov.uk/agreements/RM1557.12> accessed June 2022

[59] Crown Commercial Service, ‘Guidance: Applying to the G-Cloud framework’ (UK Government, 15 March 2022) <https://www.gov.uk/guidance/g-cloud-suppliers-guide> accessed June 2022

[60] Government of Canada, ‘Procurement at Shared Services Canada’ (30 November 2021) <https://www.canada.ca/en/shared-services/corporate/procurement.html> accessed June 2022

[61] Government of Canada, ‘Shared Services Canada launches Agile Procurement Process 3.0’ (23 March 2022) <https://www.canada.ca/en/shared-services/news/2022/03/shared-services-canada-launches-agile-procurement-process-30.html> accessed June 2022

[62] Australian Government, ‘Buy ICT’ <https://www.buyict.gov.au/sp> accessed June 2022

[63] Digital Transformation Agency, ‘New Policy replaces ICT Contract Capped Term and Value’ (Australian Government, 30 January 2020) <https://www.dta.gov.au/news/new-policy-replaces-ict-contract-capped-term-and-value#:~:text=Other%20limits%20in%20the%20Digital%20Sourcing%20Contract%20Limits,initial%20term%20cannot%20be%20longer%20than%203%20years> accessed 12 April 2022.

[64] GeBiz, ‘Guide to Singapore Procurement’ (Government of Singapore) <https://www.gebiz.gov.sg/singapore-government-procurement-regime.html> accessed 12 April 2022.

[65] GovTech Singapore, ‘3 new ways to partner with GovTech’ (Government of Singapore, 3 June 2019), <https://www.tech.gov.sg/media/technews/3-new-ways-to-partner-with-govtech> accessed June 2022

[66] IADB-Microsoft Public Procurement Paper 2020, p.7

[67] IADB-Microsoft Public Procurement Paper 2020, p.40

[68] IADB-Microsoft Public Procurement Paper 2020, p.50

[69] Government Digital Service, ‘Applying to the Digital Outcomes and Specialists framework’ (UK Government, 4 December 2015) <https://www.gov.uk/guidance/digital-outcomes-and-specialists-suppliers-guide> accessed June 2022

[70] Government Digital Service, ‘Guidance: The Crown Hosting Data Centres framework on the Digital Marketplace’ (UK Government, 21 August 2019) <https://www.gov.uk/guidance/the-crown-hosting-data-centres-framework-on-the-digital-marketplace> accessed June 2022

[71] IADB-Microsoft Public Procurement Paper 2020, p.58-59

[72] Crown Commercial Service, ‘Guidance – G-Cloud 13: what to do and when’ (UK Government, 9 March 2022) <https://www.gov.uk/guidance/g-cloud-13-what-to-do-and-when> accessed June 2022

[73] Digital Transformation Agency, ‘More about procurement and whole-of-government arrangements’ (Australian Government, 12 July 2019) <https://www.dta.gov.au/news/more-about-procurement-and-whole-government-arrangements> accessed June 2022

[74] Digital Transformation Agency, ‘Whole-of-Government Arrangements’ (Australian Government, 15 April 2021) <https://www.buyict.gov.au/sp?id=single_seller_arrangements> accessed June 2022

[75] Central Digital and Data Office, ‘Collection: Cabinet Office Controls’ (UK Government, 26 October 2021) <https://www.gov.uk/government/collections/cabinet-office-controls> accessed June 2022

[76] Government Digital Service Blog, ‘Government Digital Service – Red lines for IT Procurement’ (UK Government, 26 February 2014) <https://gds.blog.gov.uk/2014/02/26/red-lines-for-it-procurement/> accessed June 2022

[77] Digital Transformation Agency, ‘Funding for cloud’ (Australian Government) <https://www.dta.gov.au/help-and-advice/technologies/using-cloud-government/funding-cloud> accessed June 2022

[78] Asian Development Bank, ‘Cloud Computing as a Key Enabler for Digital Government Across Asia and the Pacific’ (June 2021) <https://www.adb.org/sites/default/files/publication/707786/sdwp-077-cloud-computing-digital-government.pdf> accessed June 2022

[79] OECD iLibrary, ‘OECD Digital Government Studies, Digital Government Review of Argentina’ (OECD Digital Government Studies, 25 June 2019) <https://www.oecd-ilibrary.org/sites/f95eb599-en/index.html?itemId=/content/component/f95eb599-en> accessed June 2022

[80] Tutki Hankintoja, ‘OpenProcurement.fi service’ (Ministry of Finance, Government of Finland) <https://tutkihankintoja.fi/?lang=en> accessed June 2022

[81] Department for Digital, Culture, Media & Sport, ‘UK backs digital revolution of public services at international summit’ (UK Government, 18 November 2021) <https://www.gov.uk/government/news/uk-backs-digital-revolution-of-public-services-at-international-summit)> accessed June 2022

[82] IADB-Microsoft Public Procurement Paper 2020 p.15

[83] GovTech Singapore, ‘Singapore Digital Government Journey’ (Government of Singapore) <https://www.tech.gov.sg/singapore-digital-government-journey/#:~:text=Currently%2C%2095%25%20of%20all%20transactions%20with%20the%20government,by%20the%20Government%20Technology%20Agency%20of%20Singapore%20%28GovTech%29> accessed June 2022

[84] Central Digital and Data Office, ‘Cloud guide for the Public Sector’ (UK Government, 8 February 2021) <https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector> accessed June 2022

85 Ministry of Finance, Agency for Digitisation, 'Creating a more digital Danish public sector' (Government of Denmark) <https://en.digst.dk/> accessed June 2022

86 Krostoffer Nilaus Olsen, 'Digital-ready legislation: Lessons from the Danish experience' (Ministry of Finance, Agency for Digitisation, Government of Denmark, October 2020) <https://joinup.ec.europa.eu/sites/default/files/news/2020-11/Digital-ready%20legislation%20-%20lessons%20from%20the%20Danish%20experience%20DG%20DIGIT%20webinar%20October%202020.pdf> accessed June 2022

87 Ministry of Finance, Agency for Digitisation, 'Evaluation of the effort to make legislation digital-ready' (Government of Denmark, May 2021) <https://en.digst.dk/media/24344/evaluation-of-the-effort-to-make-legislation-digital-ready-accessible-version.pdf> accessed June 2022

88 Microsoft News Center, 'Microsoft Paper Outlines Steps to Drive Nigeria's Digital Transformation Forward' (Microsoft News Center, 21 May 2020) <https://news.microsoft.com/en-xm/2020/05/21/microsoft-paper-outlines-steps-to-drive-nigerias-digital-transformation-forward/> accessed June 2022

89 Microsoft, 'Enabling a Digital Nigeria: A Position Paper of Microsoft's Vision for Digital Transformation and a Digital Economy that Works for Everyone' (2020) < https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Whitepaper-SRGCM3460.pdf> accessed June 2022

90 OECD Directorate for Public Governance, 'Government at a Glance 2021-- Chapter 10 'Digital Government' (July 9 2021) <https://www.oecd-ilibrary.org/sites/1c258f55-en/1/3/10/2/index.html?itemId=/content/publication/1c258f55-en&_csp_=10e9de108c3f715b68f26e07d4821567&itemIGO=oecd&itemContentType=book#sect-87> accessed June 2022

91 OECD Directorate for Public Governance, 'Government at a Glance 2021-- Chapter 10 'Digital Government' (July 9 2021) <https://www.oecd-ilibrary.org/sites/1c258f55-en/1/3/10/2/index.html?itemId=/content/publication/1c258f55-en&_csp_=10e9de108c3f715b68f26e07d4821567&itemIGO=oecd&itemContentType=book#sect-87> accessed June 2022

92 OECD Directorate for Public Governance, 'Government at a Glance 2021-- Chapter 10 'Digital Government' (July 9 2021) <https://www.oecd-ilibrary.org/sites/1c258f55-en/1/3/10/2/index.html?itemId=/content/publication/1c258f55-en&_csp_=10e9de108c3f715b68f26e07d4821567&itemIGO=oecd&itemContentType=book#sect-87> accessed June 2022

93 International Bank for Reconstruction and Development, the World Bank, 'Tech Savvy: Advancing GovTech Reforms in Public Administration', <https://documents1.worldbank.org/curated/en/099400004112257749/pdf/P1754970d6c6420f00ab5905f7004ba9c2f.pdf> accessed June 2022

94 Government Digital Service, 'Case Study: How ONS Changed Workplace Culture to get the best out of Cloud' (UK Government, 31 March 2020) <https://www.gov.uk/government/case-studies/how-ons-changed-workplace-culture-to-get-the-best-out-of-cloud> accessed June 2022

95 Digital, Data and Technology Profession, 'Collection: GDS Academy Courses' (UK Government, 31 January 2022) <https://www.gov.uk/government/collections/gds-academy-course-descriptions> accessed June 2022

96 Canada School of Public Service, 'CSPS Digital Academy' (Government of Canada, 13 January 2022) <https://www.csps-efpc.gc.ca/digital-academy/index-eng.aspx> accessed June 2022

97 Department of Information and Communications Technology, 'ICT Trainings' (Government of the Philippines, 2022) <https://dict.gov.ph/ict-trainings/> accessed June 2022

98 GovTech, 'The Digital Academy' (Government of Singapore) <https://thedigitalacademy.tech.gov.sg/> accessed June 2022

99 OECD, 'Digital Government Index: 2019 results' (OECD iLibrary, 14 October 2020) <https://dx.doi.org/10.1787/4de9f5bb-en> accessed June 2022

100 Cabinet Office, 'Government Digital Strategy' (UK Government, November 2012) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Stratetegy_-_November_2012.pdf> accessed June 2022

101 Cabinet Office, 'Government Digital Strategy' (UK Government, November 2012) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/296336/Government_Digital_Stratetegy_-_November_2012.pdf> accessed June 2022

102 Central Digital & Data Office, 'Cloud guide for the public sector' (UK Government, 8 Feb 2021) <https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector> accessed June 2022

103 HM Government, 'Government Cloud Strategy' (UK Government, March 2011) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/266214/government-cloud-strategy_0.pdf> accessed June 2022

104 Government Digital Service, 'How ONS changed workplace culture to get the best out of cloud' (UK Government, 31 Mar 2020) <https://www.gov.uk/government/case-studies/how-ons-changed-workplace-culture-to-get-the-best-out-of-cloud> accessed June 2022

105 Central Digital and Data Office, 'Guidance: Buying and selling on the Digital Marketplace' (UK Government, 17 November 2020) <https://www.gov.uk/guidance/buying-and-selling-on-the-digital-marketplace> accessed June 2022

106 Open Access Government, 'G-Cloud 12: Digital transformation for the public sector' (11 May 2021) <https://www.openaccessgovernment.org/g-cloud-12-digital-transformation-for-the-public-sector/110095/> accessed June 2022

107 Central Digital & Data Office, 'Cloud guide for the public sector' (GOV.UK, 8 Feb 2021) <https://www.gov.uk/government/publications/cloud-guide-for-the-public-sector/cloud-guide-for-the-public-sector> accessed May 2022.

108 Digital Marketplace, 'Supplier opportunities: NHS Test & Trace Halo Platform Support Service' (UK Government, 16 July 2021) <https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/14699> accessed June 2022

109 Chris Ferguson, 'Leading the digital, data and technology (DDaT) response to coronavirus' (Government Digital Service, UK Government, 14 September 2020) <https://gds.blog.gov.uk/2020/09/14/leading-the-digital-data-and-technology-ddat-response-to-coronavirus/> accessed June 2022

110 Crown Commercial Service, 'Guidance—Digital Outcomes: team capabilities' (UK Government, 8 February 2022) <https://www.gov.uk/guidance/digital-outcomes-team-capabilities> accessed June 2022

111 Digital Marketplace, 'Supplier opportunities: NHS Test & Trace Halo Platform Support Service' (UK Government, 16 July 2021) <https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/14699> accessed May 2022

112 Crown Commercial Service, 'Notice of Awarded Contract: Crown Hosting II' (UK Government 3 February 2022) <https://www.find-tender.service.gov.uk/Notice/003201-2022?origin=SearchResults&p=1> accessed June 2022

113 Digital Marketplace, 'Supplier opportunities: NHS Test & Trace Halo Platform Support Service' (UK Government, 16 July 2021) <https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/14699> accessed May 2022

114 Digital Marketplace, 'Supplier opportunities: NHS Test & Trace Halo Platform Support Service' (UK Government, 16 July 2021) <https://www.digitalmarketplace.service.gov.uk/digital-outcomes-and-specialists/opportunities/14699> accessed May 2022

115 Department for Digital, Culture, Media & Sport, 'Policy paper- National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy' (UK Government, 24 November 2021) <https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy> accessed June 2022

116 Department for Digital, Culture, Media & Sport, 'Policy paper- National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy' (UK Government, 24 November 2021) <https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy> accessed May 2022

117 Department for Digital, Culture, Media & Sport, 'Guidance: National Data Strategy' (UK Government, 28 April 2022) <https://www.gov.uk/guidance/national-data-strategy> accessed June 2022

118 Department for Digital, Culture, Media & Sport, 'Consultation outcome: Government response to the consultation on the National Data Strategy' (UK Government, 18 May 2021) <https://www.gov.uk/government/consultations/uk-national-data-strategy-nds-consultation/outcome/government-response-to-the-consultation-on-the-national-data-strategy> accessed June 2022

119 Department for Digital, Culture, Media & Sport, 'Guidance: National Data Strategy Forum' (UK Government, 21 March 2022) <https://www.gov.uk/guidance/national-data-strategy-forum> accessed June 2022

120 Department for Digital, Culture, Media & Sport, 'Policy paper: National Data Strategy' (UK Government, 9 December 2020) <https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#contents> accessed June 2022

121 Department for Digital, Culture, Media & Sport, 'Policy paper: 2022 cyber security incentives and regulation review' (UK Government, 19 January 2022) (the "UK DCMS 2022 Paper") <https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review> accessed June 2022

122 UK DCMS 2022 Paper

123 UK DCMS 2022 Paper

124 UK DCMS 2022 Paper

125 Department for Digital, Culture, Media & Sport, 'Policy paper: Digital Regulation: Driving growth and unlocking innovation' (UK Government, 9 March 2022) <https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/digital-regulation-driving-growth-and-unlocking-innovation> accessed June 2022

126 Competition and Markets Authority, 'Collection: Digital Markets Unit' (UK Government, 20 July 2021) <https://www.gov.uk/government/collections/digital-markets-unit> accessed June 2022

127 UK DCMS 2022 Paper

128 Department for Digital, Culture, Media & Sport, 'Policy paper: Plan for Digital Regulation: Summary of responses to the 'call for views" (UK Government, 9 March 2022) <https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/plan-for-digital-regulation-summary-of-responses-to-the-call-for-views> accessed June 2022

129 TechUK, 'How digital has reduced the Brexit burden' (16 March 2022) <https://www.techuk.org/resource/how-digital-has-reduced-the-brexit-burden.html> accessed June 2022

130 TechUK, 'How digital has reduced the Brexit burden' (16 March 2022) <https://www.techuk.org/resource/how-digital-has-reduced-the-brexit-burden.html> accessed June 2022

131 Central Digital & Data Office, 'Policy Paper: Government Technology Innovation Strategy' (UK Government, 10 June 2019) <https://www.gov.uk/government/publications/the-government-technology-innovation-strategy/the-government-technology-innovation-strategy> accessed June 2022

132 Tom Read, 'Government Digital Service: Our strategy for 2021-2024' (Government Digital Service Blog, UK Government, 20 May 2021) <https://gds.blog.gov.uk/2021/05/20/government-digital-service-our-strategy-for-2021-2024/> accessed June 2022

133 UK Government, Case Study 'How ONS Changed Workplace Culture to get the best out of Cloud' (31 March 2020) <https://www.gov.uk/government/case-studies/how-ons-changed-workplace-culture-to-get-the-best-out-of-cloud> accessed May 2022

134 Digital, Data and Technology Profession, 'Collection: GDS Academy Courses' (UK Government, 31 January 2022) <https://www.gov.uk/government/collections/gds-academy-course-descriptions> accessed May 2022

135 NHS Digital, 'GDS Academy Training Contract: A Contract Award Notice' (BidStats, 11 June 2020) <https://bidstats.uk/tenders/2020/W24/728695009> accessed June 2022

136 Central Digital & Data Office, 'Policy Paper: Government Technology Innovation Strategy' (UK Government, 10 June 2019) <https://www.gov.uk/government/publications/the-government-technology-innovation-strategy/the-government-technology-innovation-strategy> accessed May 2022

137 Department for Digital, Culture, Media & Sport, 'National statistics-- DCMS Sectors Economic Estimates 2019: Employment' (Office for National Statistics, UK Government, 30 April 2020) <https://www.gov.uk/government/statistics/dcms-sectors-economic-estimates-2019-employment/dcms-sectors-economic-estimates-2019-employment> accessed June 2022

138 Department for Digital, Culture, Media & Sport, 'Research and analysis: Assessing the UK's regional digital ecosystems' (UK Government, 30 September 2021) <https://www.gov.uk/government/publications/assessing-the-uks-regional-digital-ecosystems> accessed June 2022

139 Tom Read, 'Government Digital Service: Our strategy for 2021-2024' (Government Digital Service Blog, UK Government, 20 May 2021) <https://gds.blog.gov.uk/2021/05/20/government-digital-service-our-strategy-for-2021-2024/> accessed June 2022

[140] Tom Read, ‘Government Digital Service: Our strategy for 2021-2024’ (Government Digital Service Blog, UK Government, 20 May 2021) <https://gds.blog.gov.uk/2021/05/20/government-digital-service-our-strategy-for-2021-2024/> accessed June 2022

[141] Home Office, Digital Data & Technology, ‘Home Office DDaT 2024 Strategy’ (UK Government, 20 October 2021). <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1027402/Home_Office_DDaT_2024_Strategy_Report.pdf> accessed June 2022

[142] Department for Digital, Culture, Media & Sport, ‘Policy paper: UK digital identity and attributes trust framework - alpha version 2’ (UK Government, 6 April 2022) <https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2#contents> accessed June 2022

[143] HM Treasury, ‘Policy paper: Build Back Better: Our plan for growth’ (UK Government, 3 March 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/968403/PfG_Final_Web_Accessible_Version.pdf> accessed June 2022

[144] Cabinet Office, ‘Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy’ (UK Government, 2 July 2021) <https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy> accessed June 2022

[145] Cabinet Office, ‘Cyber Security Strategy 2022–2030’ (UK Government, 17 February 2022) <https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030> accessed June 202

[146] Department for Digital, Culture, Media & Sport, ‘Our 10 Tech Priorities’ (UK Government, March 2021) <https://dcms.shorthandstories.com/Our-Ten-Tech-Priorities/index.html> accessed June 2022

[147] Smart Nation Singapore, ‘Milestones of Singapore’s Smart Nation Story’ (Government of Singapore) <https://www.smartnation.gov.sg/about-smart-nation/our-journey/milestones> accessed June 2022

[148] Smart Nation Singapore, ‘Digital Government’ (Government of Singapore) <https://www.smartnation.gov.sg/about-smart-nation/digital-government> accessed June 2022

[149] Smart Nation Singapore, ‘Transforming SG through Tech’ (Government of Singapore) <https://www.smartnation.gov.sg/about-smart-nation/transforming-singapore> accessed June 2022

[150] GovTech Singapore, ‘Singapore digital government journey’ (Government of Singapore) <https://www.tech.gov.sg/singapore-digital-government-journey/> accessed June 2022 .

[151] GovTech Singapore, ‘Parking.sg’ (Government of Singapore) <https://www.tech.gov.sg/products-and-services/parking-sg/> accessed June 2022

[152] GovTech Singapore, ‘Moments of Life is now LifeSG’ (Government of Singapore, 8 September 2020) <https://www.tech.gov.sg/media/technews/moments-of-life-is-now-lifesg-story-so-far> accessed June 2022

[153] GovTech Singapore, ‘GoBusiness Portal’ (Government of Singapore) <https://www.tech.gov.sg/products-and-services/gobusiness/> accessed June 2022

[154] GovTech Singapore, ‘Responding to Covid-19 with Tech’ (Government of Singapore) <https://www.tech.gov.sg/products-and-services/responding-to-covid-19-with-tech/> accessed June 2022

[155] Choo Yun Ting and Prisca Ang, ‘SGFinDex: How you can check your bank, CPF accounts online on 1 platform’ (The Straits Times, 7 December 2020) <https://www.straitstimes.com/business/banking/sgfindex-7-things-to-know-about-the-new-online-tool-that-consolidates-personal> accessed June 2022

[156] Jude Chan, ‘Singapore launches trade data sharing platform to cut supply chain inefficiencies, rebuild trust’ (The Business Times, 1 June 2022) <https://www.businesstimes.com.sg/energy-commodities/singapore-launches-trade-data-sharing-platform-to-cut-supply-chain-inefficiencies> accessed June 2022

[157] Digital Transformation Agency, ‘About us’ (Australian Government) <https://www.dta.gov.au/about-us> accessed June 2022

[158] Digital Transformation Agency, ‘Digital Government Strategy’ (Australian Government, December 2021) <https://www.dta.gov.au/digital-government-strategy> accessed June 2022

[159] Digital Transformation Agency, ‘Digital Government Strategy’ (Australian Government, December 2021) <https://www.dta.gov.au/digital-government-strategy> accessed June 2022

[160] Digital Transformation Agency, ‘Secure Cloud Strategy’ (Australian Government, October 2021) <https://www.dta.gov.au/our-projects/secure-cloud-strategy> accessed June 2022

[161] Digital Transformation Agency, ‘Whole-of-Government Hosting Strategy’ (Australian Government) <https://www.dta.gov.au/our-projects/whole-government-hosting-strategy> accessed June 2022

[162] Digital Transformation Agency, ‘Digital Government Strategy’ (Australian Government, December 2021) <https://www.dta.gov.au/digital-government-strategy> accessed June 2022

[163] Australian Government, ‘About myGov’ <https://my.gov.au/mygov/content/html/about.html> accessed June 2022

[164] Australian Government, ‘Government Trusted Digital Identity Framework (TDIF)’ <https://www.digitalidentity.gov.au/tdif> accessed June 2022

[165] Australian Digital Health Agency, ‘Digital Health, My Health Record’ (Australian Government) <https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record>, accessed June 2022

[166] Australian Government, ‘My Health Record’, <https://www.myhealthrecord.gov.au/> accessed June 2022

[167] Australian Government Business Registration Service, ‘Business Registration Service’, <https://register.business.gov.au/> accessed June 202

[168] IP Australia, ‘Alex: IP Australia’s virtual assistant’ (Australian Government, 7 October 2016) <https://www.ipaustralia.gov.au/beta/virtual-assistant> accessed June 2022

[169] Department of Industry, Science, Energy and Resources, ‘Australia’s Artificial Intelligence Action Plan’ (Australian Government) <https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan> accessed June 2022

[170] Department of the Prime Minister and Cabinet, ‘Blueprint for Critical Technologies’ (Australian Government, 17 November 2021) <https://www.pmc.gov.au/resource-centre/domestic-policy/blueprint-critical-technologies> accessed June 2022

[171] Department of the Prime Minister and Cabinet, ‘New investment in Australia’s quantum technology industry’ (Australian Government, 17 November 2021) <https://www.industry.gov.au/news/new-investment-in-australias-quantum-technology-industry> accessed June 2022

Microsoft Linklaters