DATA MANAGEMENT POLICIES AND PRACTICES IN GOVERNMENT

DECEMBER 2022

AWS INSTITUTE

ADB

DATA MANAGEMENT POLICIES AND PRACTICES IN GOVERNMENT

DECEMBER 2022

AWS INSTITUTE

ADB

ISBN 978-92-9269-963-5 (print); 978-92-9269-964-2 (electronic); 978-92-9269-965-9 (ebook)
Publication Stock No. TCS220582-2
DOI: http://dx.doi.org/10.22617/TCS220582-2

Corrigenda to ADB publications may be found at http://www.adb.org/publications/corrigenda.

Notes:
In this report, "$" refers to United States dollars, "£" refers to British pound, "₹" refers to Indian rupee, and "Rp" refers to Indonesian rupiah.

ADB recognizes "China" as the People's Republic of China; "Hong Kong" as Hong Kong, China; and "Korea" as the Republic of Korea.

Cover design by Francis Manio.

Contents

Table, Figures, and Boxes

Table

Figures

Boxes

Acknowledgments

This report was prepared as part of the implementation of the Asian Development Bank (ADB) regional technical assistance, Digital Development Facility for Asia and the Pacific, which is cofinanced by the Republic of Korea e-Asia and Knowledge Partnership Fund and is copublished with the Amazon Web Services (AWS) Institute.

ADB and the AWS Institute would like to acknowledge Michael Khoo, Senior Manager, Access Partnership, as project lead and author. Contributing authors were Sim Xin Yi, Analyst, Access Partnership; and Gayathri Haridas, Manager, Access Partnership.

The preparation and production of this report was guided by Arndt Husar, Senior Public Management Specialist, Digital Technology for Development Unit, Sustainable Development and Climate Change Department (SDCC-DT), ADB; and Monique Viengkhou, AWS Institute Lead, Asia Pacific and Japan.

The peer reviewers of this report were Mark Thompson, Professor in Digital Economy, University of Exeter Business School; and Ashok Kumar, Director of Digital Government, Executive Education, School of Computer Science, Carnegie Mellon University. Additional reviews and feedback were provided by the following ADB and AWS staff: Makoto Kubota, (former) Adviser (Data Management), IT Department; Pamela Wyatt, Principal Public Management Specialist, Pacific Department; Arun Ramamurthy, Principal Infrastructure Specialist (Digital Technology), East Asia Department; Sarah Ryle, AWS Institute Senior Content Manager; and John Cann, AWS Head Market Development, Asia Pacific and Japan.

Terry Erle Clayton, Consultant, ADB, copyedited the draft paper; Lawrence Casiraya proofread the draft paper; Francis Manio created the cover art; and Prince Nicdao typeset the final publication. Carmela Fernando-Villamar, digital technology officer, SDCC-DT; and Genny Mabunga, Senior Operations Assistant, SDCC-DT, provided valuable administrative support.

Executive Summary

Effective data management is a top priority for governments as it plays a key role in unlocking the value of data.* By opening access to public sector data sets, governments create opportunities for innovation and entrepreneurship by nongovernment actors to identify and respond to evolving societal needs that can enhance the quality of life.

According to the World Economic Forum, public sector data sharing is estimated to create socioeconomic benefits worth between 0.1% and 1.5% of gross domestic product. The more data are connected, the higher its utility and value. Positive knock-on effects are created when data are combined with other data and indications are that sharing data and increasing access will drive up its value for all stakeholders.**

Governments are among the world's largest producers and largest users of data as they aim to deliver better and more efficient public services. Data analytics can be leveraged to track, evaluate, and provide real-time insights on the flows of public resources (e.g., tracking gender equality, leakage or waste of resources, or the spread of viral infections) or trigger a response by a public service provider (e.g., in the case of a disaster or as a response to peak demand in public transport). Leveraging data can minimize the waste of resources and improve public outcomes.

However, maximizing the potential of public sector data requires robust frameworks governing the collection, storage, and use of data to ensure data privacy and security. Given the complexity of the subject and the rapid developments in digital technology, many governments struggle with the design and implementation of data governance and management frameworks. Challenges include a low level of awareness and understanding of the necessary frameworks and standards, inadequate financial and human resources, and low levels of coordination across agencies and ministries within the same country.

The good news is, that despite these challenges, many governments in Asia and the Pacific have embarked on policy initiatives and regulatory reforms that demonstrate a desire to actively manage their data, facilitate sharing, and set up much-needed regulatory frameworks. This publication has been developed to aid governments in developing holistic approaches to conceptualizing, creating, and implementing data management policies and practices. These are coupled with case studies and grouped into three main sections:

---

* Organisation for Economic Co-operation and Development (OECD). 2019. *The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies*.

** World Economic Forum. 2021. *Articulating Value from Data*.

- **identifying quick wins** to generate stakeholder buy-in and facilitate wider societal acceptance;
- **scaling up data use** to maximize the utility of available data resources; and
- **building governance** mechanisms to ensure that data use is regulated, secure, and transparent.

Examples illustrate how governments have implemented their own approaches, and more comprehensive case studies cover the data management and digital transformation journeys taken by three countries—Indonesia, Japan, and the Republic of Korea. As there is no one-size-fits-all approach, these examples and case studies are meant to demonstrate some of the best practices that reflect challenges and solutions developed across a wide range of economies to build robust data management frameworks.

The ability to harness the transformative effects of data has become a key determinant of a government's ability to make effective decisions and meaningfully engage with stakeholders. Coordinated and robust data management practices are essential to reap these benefits for government:

- **High-quality policy making** that is evidence-based and guided by the targeted analysis of data sets from across a variety of agencies, allowing for well-coordinated approaches to social, economic, and administrative issues.
- **Improved coordination across agencies** through the development of harmonized internal data systems and frameworks for information sharing means more holistic programs and stronger inter-agency partnerships. This coordination further helps to minimize redundancy and promote interoperability at a whole-of-government level. Intelligent systems can avoid failure demand, i.e., unnecessary demand on public services created by a lack of coordination or intelligent action.
- **Powerful digital government platforms**, known as e-government platforms, can address the increasingly diverse needs of citizens and ensure that government initiatives are effectively delivered to those in need. This strengthens citizen engagement, leading to more efficient and equitable service overall.
- **Harmonized internal data systems** can be centrally coordinated across agencies to reduce duplicated labor and inefficiencies, and promote interoperability at a whole-of-government level which can be managed holistically in accordance with international best practices regarding format, security, and other factors.

Evidence-based policy making based on rigorous analysis of data sets has become a baseline capability of effective government agencies and projects. As citizens increasingly interface with private sector digital services, they expect more seamless, secure, and anticipatory digital services which governments create and maintain.

Governments that are unable to develop cohesive approaches to data management risk being left behind, as other nations progressively deploy data-driven approaches to governance and growth. During the coronavirus disease (COVID-19) pandemic, for example, countries that deployed data-based approaches to track and respond to the spread of the virus alongside data-powered digital services for contactless interactions fared better in containing new infections, and so had more capacity to develop strategic responses.

However, while many governments around the world have acknowledged the importance and value of leveraging data, many still face the challenge of matching their existing infrastructure and systems with the growing demand for data management frameworks, and governments still struggle to develop the necessary foundations to implement them.

Some governments have uncoordinated legacy systems that have drastically diverged to the point that they require costly efforts to bring agencies into alignment. Other governments lack substantive experience with any data management systems at all, due to limited exposure or ossified systems resistant to digital transformation. Others do not have the necessary regulatory frameworks to ensure that data management principles are underwritten by appropriate enforcement regimes. To gain the public trust and limit the risks and potential for misuse, these issues are critical as they determine the management of sensitive data including digital identification and census data.

Developing holistic data management practices is a journey that government institutions may embark upon when challenged to become more proactive, reduce friction in service provision, and be less compartmentalized and more consent-based. The first step would be to recognize the importance of data and make a firm commitment toward implementing a coordinated, robust, and holistic data management policy. This would be followed by a clearly articulated change management process led by an empowered agency to ensure this commitment is followed by the appropriate changes necessary for governments to implement such a policy. With the increasing importance of data in everyday life, however, this is not a challenge that governments will be well served in shying away from or addressing with half-measures. Strong data management is critical for building excellence in governance.

Managing Public Sector Data

1

This section introduces the importance of data by highlighting the benefits and examples of how data are being used across sectors and in different economies. It also introduces the definition of data management alongside key concepts and underscores the potential barriers and challenges that governments face when implementing an appropriate data management approach.

Introduction

Data are the cornerstone of digitalization today. This involves the use of digital technologies to transform business models and digital government services to improve efficiency and productivity. Data underpin access to products, services, and activities that have become core to economic growth in the Asia and Pacific region and across the world. Access to plentiful supplies of data is the main prerequisite for value creation in the global digital economy, as it is through the analysis and processing of raw data that actionable digital intelligence is created.[1] Companies which have been able to harness the power of data have been able to design more robust and user-friendly digital tools and services to connect communities, build marketplaces, and better address social gaps in health care and education.

Just as commercial service providers across a variety of sectors have sought to leverage digital technologies to provide facilities such as online banking to make using their services more convenient, so too do governments seek to transform how citizens access government services by implementing e-government programs. Access to large amounts of well-managed data is necessary to ensure the delivery of citizen services can be optimized to the needs of a country's population and context.

Governments benefit from regular and sustainable access to data sets that are often unmatched in both breadth and granularity. Census data and other information collected during normal government functions are resources that can be harnessed for the public good. The vast quantity of collected data is set to increase again as government-to-citizen interactions increasingly move online. The International Data Corporation (IDC) has forecast that global data creation and replication will experience a compound annual growth rate of 23% over the 2020–2025 period (Box 1).[2]

[1] United Nations Conference on Trade and Development (UNCTAD). 2021. *Digital Economy Report 2021*.

[2] *Businesswire*. 2021. Data Creation and Replication Will Grow at a Faster Rate Than Installed Storage Capacity, According to the IDC Global DataSphere and StorageSphere Forecasts. 24 March.

Box 1: Australian Bureau of Statistics Operates 2021 Census on the Cloud

In 2021, the Australian Bureau of Statistics (ABS) ran the Australian Census on the cloud for the first time. The census is the most comprehensive snapshot of the country and includes around 10 million households and over 25 million people. Some of the topics covered in the census data included income and work, health, education, and cultural diversity. The statistics are used by government, business, and community organizations to make important decisions about transport, schools, health care, roads, and buildings, and to help plan local services for individuals, families, and communities.

For the 2021 Census, the ABS engaged PwC Australia to create a robust Census Digital Service (CDS) hosted on Amazon Web Services Institute that would enable them to manage the massive web traffic generated by millions of users. The CDS scaled to deliver forms to over 2.5 million people in 24 hours on Census Day. At peak time, over 142 forms were submitted per second. There were also sufficient security measures in place to successfully block traffic from over 130,000 malicious IP addresses during the census period.

Aside from the CDS, the ABS delivered three more systems to support census operations on the cloud:

(i) Operational Insights, a serverless data lake that provided near real-time insights to ABS on census operations related to the number of submitted forms, the progress of census field workers, and a breakdown of types of queries from the public.

(ii) Paper Form Request Service, an automated platform that enabled people to request paper forms, collectively saving thousands of hours of wait time in the Census Contact Centre.

(iii) Natural language processing system, to analyze feedback from customer forms.

With such a wealth of data come challenges. For example, government data collection is often a purpose-driven process, with agencies collecting data for specific purposes, and storing or processing it according to principles developed in an uncoordinated fashion. This means that government data are plentiful but fragmented, which seriously limits its usability for e-government processes beyond the purposes for which it was collected. In Singapore, the government treats data as a whole-of-government asset and its current Government Data Architecture (GDA) operates on the principle of data sharing by default. However, in practice, data sharing still takes several months of negotiation and maneuvering as the data are often collected for individual agency use and not for cross-government use.[3] Furthermore, while the GDA provides data security safeguards, there must be a consistent treatment of sensitive data necessary for inter-agency data sharing.

For governments to make effective use of their massive data assets, a holistic data management policy and an enabling regulatory environment are required.

Case studies highlight specific data management processes. Through showcasing these best practices, this report draws on lessons learned by public sector agencies across the world to identify common themes and optimal approaches to successful data management and utilization.

[3] D. Lim Yew Mao. 2019. Bringing Data into the Heart of Digital Government. Civil Service College Singapore. 8 August. https://www.csc.gov.sg/articles/bring-data-in-the-heart-of-digital-government.

Primary interviews with key public sector and regulatory stakeholders were conducted to provide a more detailed understanding of the challenges faced and solutions undertaken by various public sector agencies across the Asia and Pacific region. This enabled the researchers to incorporate their views about challenges they faced and addressed in advancing their data management initiatives. Data management practices across a variety of countries were reviewed to ensure that the recommendations made in this report are relevant and implementable by the widest possible range of economies. This report examines select countries to highlight specific approaches taken in their data management journey.

Throughout the report, we have referenced various types of data. The broad definition of these concepts aligns with legislation in other countries:

- **Personally identifiable information:** Any information about an individual, including those that can be used to distinguish or trace an individual's identity, such as name, social security number, date of birth, or biometric records.[4]
- **Open data:** Digital data made available with the technical and legal characteristics necessary for it to be freely used, reused, and redistributed by anyone, anytime, anywhere.[5]
- **Proprietary data:** Data owned by an individual or organization which are deemed important enough to provide a competitive advantage. This data can constitute trade secrets or privileged or confidential commercial or financial information.
- **Anonymized data:** Data are considered anonymized when individuals are no longer identifiable.
- **Data portability:** Provides restricted access through which data holders can provide customer data in a commonly used, machine-readable structured format, either to the customer or to a third party chosen by the customer.[6]

This report will address as wide an array of dimensions to public sector data management as possible. Such dimensions may include targeted improvements to existing practices or guidelines; principles of regulatory innovation; or the adaptation of best practices around data governance, data standards, data sharing, data privacy, trust, and cybersecurity.

4 International Association of Privacy Professionals. *Personally Identifiable Information*.

5 Open Data Charter. *International Open Data Charter*.

6 OECD. 2019. *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*.

Benefits to Public Sector Outcomes

The coronavirus disease (COVID-19) pandemic drove a surge in migration to digital services. In Southeast Asia, an estimated 36% of all digital service consumers are new, having participated in a 'flight to digital' because of the COVID-19 pandemic.[7] Surveys indicate that 94% of new digital service consumers intend to continue using digital services after the pandemic, suggesting this development, and any corresponding rise in the uptake of digital government services, will not be temporary. This shift to digital could present governments with opportunities to simultaneously improve the quality and reach of government services, while also reducing costs associated with human resources and administrative inefficiencies through digital applications and platforms.

Putting in place appropriately robust practices for public sector data management will be vital to allowing governments to better meet emerging demands on their e-government systems and enable them to unlock organizational and managerial efficiencies with whole-of-government and whole-of-society implications. The growth in the adoption of e-government systems worldwide has resulted in use-cases for e-government services to grow more diverse, even as their effectiveness comes under greater public scrutiny. The 2020 Digital Government Survey[8] found that while government services are getting more complex and despite governments ramping up digital services, citizen expectations across 36 surveyed countries regarding the quality of government services are also rising, causing overall user satisfaction to remain relatively static (footnote 8). Effectiveness and impact through the use of data extends beyond government services to other public services such as health care, education, and transport with myriad benefits to cost reduction and gross domestic product (GDP) growth. The Asian Development Bank (ADB) report *Harnessing the Potential of Big Data in Post-Pandemic Southeast Asia* projected annual cost reductions of $9.4 billion in Southeast Asia's public health-care sector by way of reducing hospital visits, length of patient stays, and number of procedures through the efficient use of data-reliant remote monitoring systems by 2030 (footnote 8). Data-driven innovations in the education sector could allow for the deployment of personalized learning applications and online analytics-based job-matching platforms, which are projected to contribute $77.1 billion annually to the GDP of Southeast Asian countries by 2030 as well.

Opening access to public sector data to businesses, academics, and private citizens can lead to the organic development of tools and services that can complement public infrastructure without compromising data privacy and security. Public transport systems collect large amounts of data from pre-loaded transit cards, with London Transport (Transport for London) in the United Kingdom reportedly sitting on a trove of data worth at least £116 million a year, taken from the time saved by tourists, commuters, and residents through the use of its data.[9] London Transport opted to provide direct access to these data reservoirs (with privacy by design) to private developers, facilitating the creation of applications that address issues like traffic congestion and public transport commute routing. The open data initiative only published public data, and private data such as transit card transactions made when using public transport are being kept securely.[10]

---

7 Google, Temasek, and Bain & Company. 2020. *e-Conomy Sea 2020*.

8 Boston Consulting Group. Digital Government.

9 C. Neilan. 2016. Open data: London is streets ahead when it comes to helping commuters plan their journey—but we mustn't become complacent. *City A.M. Limited*. 12 May.

10 J. Card. 2015. Open data is at the center of London's transition into a smart city. *Guardian News & Media Limited*. 3 August.

Another example is integrating crowdsourced data with data from government agencies. In Jakarta, citizens are using social media to report and obtain information on extreme weather conditions. The University of Wollongong's PetaBencana platform uses the power of social media combined with government agency validations to gather, sort, and display real-time information for disaster risk management. It produces city visualizations of disasters in Indonesia that harnesses the heightened use of social media and instant messaging during emergency events to gather confirmed situational updates from street level, in a manner that removes the need for time-consuming data processing. The tool integrates crowdsourced data with data from other origins, including government agencies and water-level-sensing devices, thereby enhancing data accuracy. The cloud enables immediate collection and analysis of data from various sources and transfer for mapping and decision-making (Box 2).

Box 2: United Kingdom Department for Transport Adopts Cloud for Rail Network Operations

The Department for Transport (DfT) is a government body that seeks to support the United Kingdom (UK) transport system to help people and goods move around the country. DfT's ability to respond to queries on the vast volume of data they hold is crucial to informing the way transport services across the country are run. For rail, which provides some of the UK's most important transport infrastructure, these queries were run by DfT's rail technical and data management team on the Latest Earnings Networked Nationally Overnight (LENNON) application. However, the DfT is unable to make best use of this trove of data due to technical limitations, leaving it dependent on others to answer queries for them.[a]

To address these issues, DfT migrated the LENNON system to the cloud, allowing it to run multiple data queries simultaneously on the system, with queries returning visualized results 20 times faster than before. According to the department, processing speeds have fallen dramatically. Where it used to take hours to execute a query, it is now taking less than 20 seconds. This has led to better, more timely data insights that can be used to inform decisions made about the UK's rail network.[b]

[a] Global Government Forum. 2022. From inflation to injections: how governments can use cloud technology to provide real-time insights.
[b] CTS. 2019. Driving Digital Transformation with the Department for Transport and Google Cloud.

Another means of leveraging crowdsourcing is by making available data collected by governments for the public to access and use. In the Republic of Korea, the open government data portal is established through the data.go.kr platform that provides a single access point to open data from the Korean government.[11] The availability of public data offers opportunities for private and research sectors. For example, through the Open Fiscal Data platform, the public gains access to open financial information, including tax history. Open data also enables the government to improve the transparency and reliability of budget operations. In addition, the financial sector may leverage public data to facilitate the management of government bonds, compare interest rates on deposit loans, and create new insurance-related financial firms.[12]

[11] OECD. OURdata Index: 2019 (Republic of Korea).
[12] UNESCAP. 2020. Open Government Data Policies and Practices in the Republic of Korea.

As well as facilitating the delivery of new citizen services and improving the delivery of existing ones, prudent management of data resources will allow governments to respond with greater agility to societal and economic developments they detect in the data they collect. The increasing rate of digital interactions that accompanies the proliferation of e-government services will undoubtedly generate even richer sources of raw data that can be analyzed to further improve the management of public utilities and underwrite evidence-based decision-making at the national, regional, and municipal levels. For example, in the People's Republic of China, the Guangxi government uses big-data-driven performance management of government programs to promote public sector innovations, such as developing technology platforms for poverty targeting and investment tracking.[13] In contrast, poor data management can result in inefficiency and incur unnecessary costs. Based on IBM estimates, poor-quality data cost the United States (US) economy $3.1 trillion per year, which is around 15% of GDP.[14] Poor storage practices and inadequate documentation have especially far-reaching economic consequences, as additional resources must be deployed to clean the data for use or ascertain when or how it originated before it can be meaningfully analyzed. Negligence in this area can also have security implications as poorly defined or ill-enforced data classification regimes may result in sensitive data being misclassified and granted inadequate protection or encryption, leading to data losses and a consequent deterioration of public trust in government data practices.

On a positive note, awareness of the need for appropriately robust data policies is growing, especially considering the COVID-19 pandemic and the accompanying 'flight to digital.' Seventy-five percent of surveyed government chief data officers in Australia, India, New Zealand, and Singapore believe their governments should have invested in data initiatives before the onset of the pandemic.[15]

Defining Data Management

Following the illustrations on the benefits of data begs the question of what data management actually refers to. This publication views data management as a wide range of practices and methodologies, including data collection, data organization, data classification, data access, data storage, data availability, data purging, and data protection, to help organizations better leverage their data for decision-making. In short, data management ensures that the quality of data is captured, processed, stored, and shared appropriately. This enables secure access to data by the relevant personnel or department at the right time. At the same time, proper data management also involves data purging, which allows individuals to request the deletion of their data when it is no longer necessary. This right to erasure is borrowed from the European Union's General Data Protection Regulation (GDPR) and is implemented in some countries like Indonesia and India. The development of sound data management would, therefore, involve strategies and policies on data organization, architecture, and infrastructure.

This aligns with definitions adopted by authoritative international organizations concerned with data management. The Data Management Association defines data management as describing the processes used to plan, specify, enable, create, acquire, maintain, use, archive, retrieve, control, and

[13] L. Goh et al. 2019. Taking the pulse of digital government in China. *World Bank Blogs*. 30 October.

[14] C. Lees. 2021. The real cost of poor data management. *Data Clan*. 5 May.

[15] Omdia. 2021. *Emergence of the Public Sector Chief Data Officer in Asia Pacific*.

purge data.[16] Alternatively, the International Organization for Standardization (ISO)/IEC Technical Report 10032:2003 on a Reference Model of Data Management defines data management as including the description, creation, modification, use, and control of data in information systems.[17]

This publication considers that a key indicator of effective data management is the interoperability of managed data. This conforms with conclusions reached by organizations such as McKinsey, which highlighted interoperability as a key predictor of effective data use in the public sector.[18] Interoperability in this context will be understood as the degree to which data collected, processed, and stored by a single agency can be meaningfully accessed and analyzed by other entities, whether these be other agencies or businesses and private individuals. In some circumstances, such as when regional alignments on data policy and data-sharing arrangements are being sought, cross-border interoperability may also be a prioritized element of data management.

Productive data management policies for government would thus provide guidelines on how to use data assets across public sector agencies and how this data would be accessible to members of the public, including private sector, academic, and individual users. Effective policies would also facilitate coordination regarding data issues to ensure that lines of communication are open between agencies and organizing entities, with the aim of promoting whole-of-government and eventually whole-of-society alignment on data management practice.

Potential Barriers and Challenges

Many governments recognize the importance of data management, but struggle with how best to implement appropriate data management policies in cost-efficient and non-disruptive ways. Compounding these struggles are outdated management philosophies and inefficient bureaucratic processes, which can prevent development and implementation of necessary data management policy changes in a timely and efficient manner.

The New Zealand government surveyed 270 public sector organizations in 2019–2020 and found that the biggest challenges to data management included a lack of understanding of its importance, poor communication across functional groups, and inadequate data management during project planning.[19] The Government of Australia reported in 2015 that some departments, such as the Australian Taxation Office, the Department of Human Services, and the Department of Social Services, had concerns regarding the privacy of some data, which hampered these departments from pursuing efforts to more widely publish or share the data even with other departments.[20]

[16] T. Olavsrud. 2021. Data Governance: A Best Practices Framework for Managing Data Assets. *CIO*. 18 March.

[17] International Organization for Standardization. ISO/IEC TR 10032:2003 Information technology Reference Model of Data Management.

[18] A. Domeyer et al. 2021. Government data management for the digital age. McKinsey & Company. 20 September.

[19] T. Koe. 2019. *Finding Report: Survey of Public Sector Information Management 2019/20*.

[20] Government of Australia, Department of the Prime Minister and Cabinet. 2015. *Public Sector Data Management*. Barton.

Many government agencies across the region also continue to grapple with data silos, which are often the legacy of an analog or paper-based filing system that was simply transferred online in an uncoordinated manner as the use of computers became ubiquitous. As more systems and information are digitalized in the emerging economies of the Asia and Pacific region, data coordination issues continue to remain a secondary concern at best for many agencies. This lack of prioritization will lead to more data being siloed, which may necessitate higher capital expenditures down the line to rationalize the data whenever data management becomes a priority.

Harmonizing data across levels of government is also a major consideration, especially for governments with developmentally diverse regional or municipal divisions. Federally or nationally mandated data management priorities may not be adequately resourced or prioritized in parts of the country which are less connected than others. Countries like Indonesia, where provincial governments report uneven rates of internet connectivity and access to digital resources, have predictably indicated difficulties in promoting alignment on data issues at the provincial and municipal levels.[21] Increasing awareness and aligning understanding across agencies and at the local level is thus fundamental and education is critical to assure agencies of the benefits of data harmonization in performance efficiency.

[21] OECD. OECD Open Government Review: Indonesia (2016 Highlights).

Road Map for Public Sector Data Management

2

This section suggests how to approach framing a data management policy for government by identifying common elements when considering a public sector data management road map. This includes establishing a strategic vision which articulates the objectives and commitments alongside establishing the necessary governance mechanisms, and the importance of identifying quick wins before scaling up the use of data.

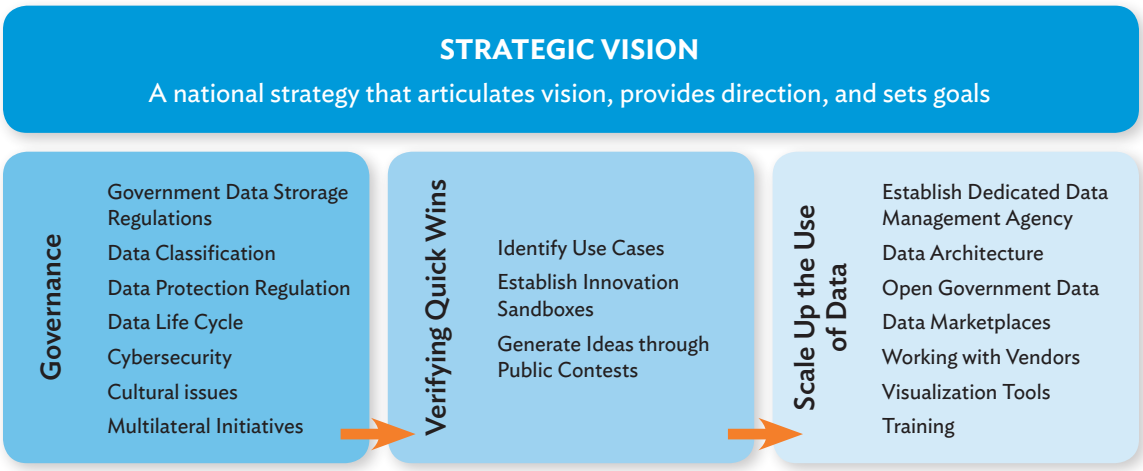
Best Practice Framework

Standardized frameworks and learning from different government systems does not mean a one-size-fits-all prescription for data management. A government that needs to overhaul legacy systems implemented in earlier stages of digitalization will have different priorities from one which has not yet embarked on digitalization. Questions of technical maturity, financial resources, and the availability of skilled professionals are also considerations that will determine where a country's data management priorities lie.

Nevertheless, this publication identifies approaches to data management which can be considered universal and which may be pursued in different ways to improve data management practices regardless of where a government is on their data management journey. It will also illustrate how these approaches can best be developed and implemented using examples of successful applications in other jurisdictions. These approaches and the general structure of this publication are illustrated in the road map in Figure 1.

This road map first recognizes that at the heart of every government's data management journey is a strategic vision that provides a necessary overarching direction. Data governance policies are important mechanisms to facilitate the provision of clear mandates for data sharing and help reassure data subjects of the security of data collection, use, and storage. The identification and facilitation of quick wins can subsequently secure buy-in from stakeholders. With buy-in, it becomes easier to deploy strategies that scale up the use of data.

Figure 1: Building Blocks of a Data Management Journey



Source: Authors' elaboration.

Establishing a Strategic Vision

Effective data management often begins with the articulation of a strategic vision at the highest levels of government. Such strategic visions are usually implemented through a national strategy, framework, or a master plan, which commits to the observance of more effective data management practices, often as part of a wider commitment to the promotion of government digitalization and the development of e-government capabilities.

These documents usually highlight the desired impact of data management within the public sector and map benchmarks and goals that agencies can work toward to achieve the vision. This functions as a signal to the wider bureaucracy that the data management agenda has received institutional priority and will be accompanied with appropriate funding and enforcement mechanisms.

Governments also need to have a sense of urgency that, amid increasing digital disruption, investments in data are aligned with the government's objective to deliver better public services to society. This point may also be accommodated through the strategic vision. It should be at the government's attention that the application of data in the public sector is aimed at generating public value, and the application of good data management has the potential to provide more efficient, effective, and trustworthy public services.[22]

Investments in data may encourage governments to adopt a data-first approach. When such huge volumes of data are accumulated and with proper data management in place, a government can use the data to adopt predictive modeling in their decision-making process. Predictive modeling could be

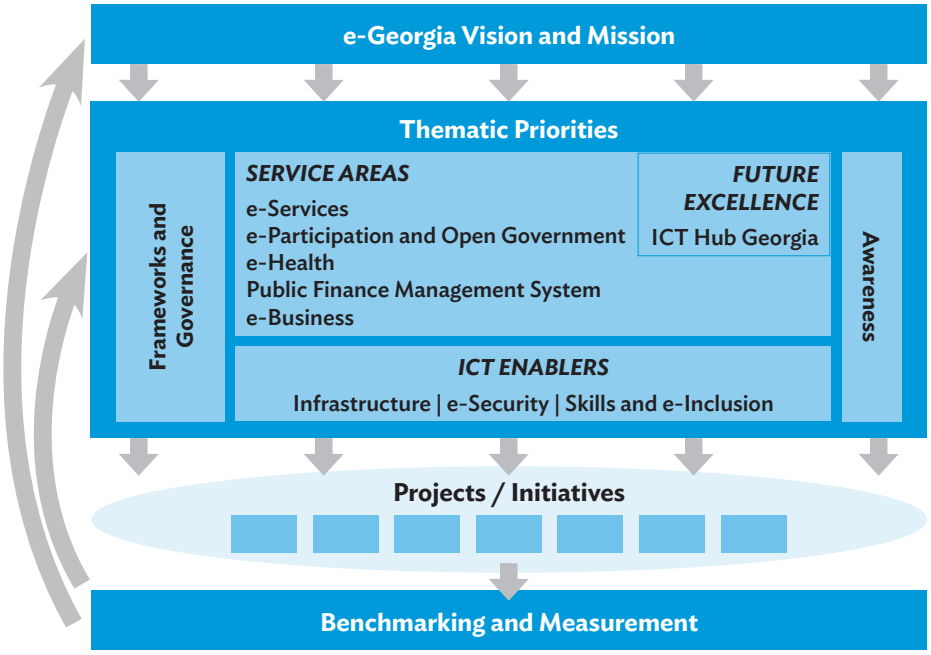
[22] OECD. 2019. *The Path to Becoming a Data-Driven Public Sector*.

the key to transforming public services to be more resilient to changes.[23] Identification and prediction of potential changes allows predictive modeling to prepare their services accordingly. This, in turn, would promote anticipatory thinking that is able to envision future scenarios to enable the public sector to become more foresighted and data-driven (footnote 23).

The deployment of a plan must be seen as only the beginning of a process which must be continually built upon and invested in to achieve meaningful outcomes. For example, Georgia's public service strategy, A Digital Georgia: e-Georgia Strategy and Action Plan 2014–2018, demonstrates how a strategic vision can catalyze meaningful digital reform (Box 3).[24]

Box 3: The e-Georgia Strategy and Action Plan 2014–2018

This strategy outlines Georgia's vision to build a more efficient and effective public sector by offering integrated, secure, and high-quality e-services, and ultimately enabling information and communication technology (ICT)-driven sustainable economic growth.



ICT = information and communication technology.

Source: N. Gagnidze and N. Goderdzishvili. 2017. *Development Path of Digital Georgia: From eGovernance Frameworks to eGovernment Initiatives*.

continued on next page

[23] Open Access Government. 2022. How Predictive Modelling Can Future-Proof the Public Sector. 17 June.

[24] B. Krabina et al. 2017. *Digital Georgia (E-Georgia Strategy and Action Plan 2014-2018)*.

Box 3 *continued*

The strategy laid out priorities for creating frameworks and governance, prioritized service areas, awareness creation, and ICT enablers. These eventually led to specific projects and initiatives centered on data management, which were informed by benchmarking and assessment activities. The Data Exchange Agency (DEA), which was set up in 2009, supported electronic data exchange by coordinating activities among various ministries. The DEA also assumed the role of the Georgian Governmental Gateway (3G), and focused on information and cybersecurity policies.[a]

Catalyzed by the e-Georgia Strategy and Action Plan 2014–2018, the Georgian government sought to leverage data for its reforms, driven by a strong desire to enhance transparency and efficiency by weeding out corruption and improving interoperability and coordination across government departments. Legislative processes in Parliament benefited from discussions between the development and technical teams who generated new ideas and use-cases, seeking inputs from lawyers and legal teams to help shape the necessary legislative changes.

It was important to developing in-house capabilities to create the necessary data management and digital systems by focusing on internal capacity building and implementing best practices derived from the experience of governments around the world.

> "When we started, [...] experts from Estonia and other countries shared their knowledge and ideas, such as on tax digitalization [...]. But within two to four years, we identified a lot of internal capacities and moved leaders of reform from one agency to another to drive change within the agencies. Along the way, they gained experience in driving these reforms, such as implementing e-filing systems for each agency. It [became] hard to find international experts who had better experience than the local experts."
>
> ***Irakli Gvenetadze***
> *CEO of LTD Digital Transformation Center;*
> *Ex-Chairman of LEPL Data Exchange Agency of Ministry of Justice of Georgia (2010–2017)*

Source: Interview with Irakli Gvenetadze, 21 January 2022.

Following the success of the e-Georgia strategy, the more recent Georgia 2020 Social Economic Development Strategy has outlined several target areas to build on progress made under the previous strategy, aiming to enhance the digital ecosystem, including high-speed broadband internet, e-literacy and capacity building, innovation and high-tech, and e-government.

[a] Developmentaid. Data Exchange Agency.

Other examples of national strategies guiding government data management

Every successful public sector data management policy begins with a clear national strategy. However, there is no one-size-fits all approach to implementing a strategy, nor should there be, as different governments should develop and prioritize their objectives based on what is important and relevant to them. The following examples demonstrate where different governments have focused their approaches to highlight different areas of prioritization (Box 4).

Box 4: Examples of National Strategies Guiding Government Data Management

- In 1994, the **Government of Estonia** created the Principles of Estonian Information Policy, which has served as a vision for government information technology (IT) development. This program allotted 1% of national GDP to state-funded IT development and served as an example of how creating a master plan could benefit overall government data management implementation.[a] This resulted in the Tiigrihüpe, or Tiger Leap, which has resulted in the e-Estonia'initiative, whereby the government has sought to enable digital solutions for every possible citizen interaction with the state. Today, Estonia is well-known as a highly digitalized economy which has 1.3 million citizens, plus 90,000 virtual residents (known as e-residents) from 177 states, who have founded approximately 20,000 new companies.[b]
- In 2009, the **Government of India** launched Aadhaar, the largest biometric identity program in the world. Aadhaar has stored information on nearly 1.2 billion Indian citizens and residents, which is close to 15% of the global population, including over 99% of all Indian adults. Each Aadhaar recipient receives a unique 12-digit identification number, and submits their photo and biometric data in the form of fingerprints and iris scans. The government uses the Aadhaar program to provide unique identification of citizens, allowing them to deliver citizen services effectively.[c] For instance, the use of Aadhaar is extensive, including the provision of direct benefit transfers such as subsidized food grains, the creation of millions of bank accounts to those unbanked, and linking to income taxes.[d]
- The **Government of New Zealand's** Data Strategy and Roadmap seeks to better integrate the government's data management systems and provide strategic direction across departments and ministries.[e] The strategy and road map were conceptualized as living documents, allowing for adjustments as implementation progresses or when new systems are necessary.[f] As part of these reforms, New Zealand's government has also appointed a "chief data steward," whose role is to further the use of data and oversee the closer integration of data into government services.[g]
- The **Government of Vanuatu** published a National Strategy for the Development of Statistics, which was led by stakeholders in the Vanuatu National Statistical System (VNSS) with funding and technical assistance from Paris21 and the SPC.[h] The strategy outlines data development actions aimed at improving the statistical information base relevant to these priority areas. It involved extensive consultations with a wide range of stakeholders including government agencies, provincial governments, research organizations, and nongovernment organizations. The VNSS identified common factors unifying effective data management processes and is now leveraging this knowledge to develop its approach to government data management.

[a] e-Estonia.
[b] BNS. 2021. 2021 saw as many new e-residents as births in Estonia. *Estonian National Broadcasting*. 29 December.
[c] OECD. 2018. *Case Study Aadhaar India*.
[d] The Hindu. Aadhaar mandatory for availing subsidised foodgrains from PDS.
[e] Data.govt.nz. The Government Data Strategy and Roadmap.
[f] Data.govt.nz. Government Data Strategy and Roadmap 2021.
[g] Data.govt.nz. Government Chief Data Steward (GCDS).
[h] Government of Vanuatu, Vanuatu National Statistics Office. 2021. *Vanuatu National Strategy Development Statistics*. Port Vila.

The strategic vision needs to be accompanied by an effective change management methodology, as implementing change in governments is often challenging, particularly if it involves implementing new systems and programs, such as digitalizing older processes and requiring staff to retrain or modify their behaviors. Change management is crucial in realizing the strategic vision.

Governance

The existence and nature of data governance mechanisms are key to governments' considerations. These mechanisms, which include data protection laws, cybersecurity regulations, and data classification standards, among others, govern the legal status of data and the conditions under which they are stored and processed and are often some of the most directly impactful means by which governments can affect how their jurisdictions interact with data.

Robust governance frameworks are necessary to protect the interests of citizens, while also ensuring that businesses are not excessively curtailed in their efforts to innovate with data. In addition, data governance should be conceptualized in a way that ensures regulations are fit-for-purpose, proportionate to the present and future needs of society, and reflective of a realistic understanding of existing use-cases and implementation options.

A robust data governance framework relies on appropriate data storage regulations, data classification systems, data protection regulations and cybersecurity, data life cycle, awareness of cultural factors, and other multilateral initiatives. In practice, having these features will ensure that governments can be custodians of data generated by citizens and businesses and can use it to benefit society.

This publication will refer to terms codified under the European Union's General Data Protection Regulation (GDPR) in categorizing entities associated with data as follows:

- **Data subjects** will refer to individuals and entities which originated data and can be in some way associated with it.
- **Data controllers** will refer to individuals and entities that decide why and how to process data.
- **Data processors** will refer to individuals and entities which process data on behalf of controllers, acknowledging that processors and controllers can be the same entity.

There are also important data governance players within an organization that have specific roles and responsibilities:

- **Chief data officers:** Responsible for the use and governance of data across the organization to drive business outcomes.
- **Data stewards:** Play a critical role in ensuring that the data are of high quality and are responsible for ensuring the classification, protection, use, and quality of that data.
- **Data custodians:** Responsible for implementing and maintaining security controls for a given data set to meet the requirements.

Government Data Storage Regulations

To promote interoperability and facilitate cross-border data flows, governments are encouraged to observe global best practices by adopting international standards on data storage and management. Doing so will ensure that government data management practices do not develop in isolation but within a holistic, peer-reviewed framework that is regularly updated to reflect changing circumstances and calibrated using a wide range of international expert input and practical experience.

Adoption of these standards at a whole-of-government level would facilitate harmonization of basic standards across agencies, while also ensuring that management methodology and security practices are aligned with international expertise. Uniform implementation of such standards on data storage may allow government agencies to build data management capacity and scale e-government initiatives more effectively. Furthermore, observation of these standards and adherence to relevant incident mitigation guidelines can aid in the management of security incidents and even lead to the recovery of lost data.

The ISO's Reference Model of Data Management, ISO/IEC TR 10032:2003, is considered an authoritative baseline international standard on data storage (Box 5).

Box 5: Standards for Data Management

Globally, the International Organization for Standardization (ISO) consolidates the register of standards, creating common and freely available standards for data management in telecommunications, security, business continuity, and information technology (IT) governance.

ISO also develops core standards for the management of electronic data and interfaces with many other organizations such as the Internet Engineering Task Force (IETF). IETF sets core standards for data exchange over the internet, as well as regional and local standards bodies. ISO also works with the World Intellectual Property Organization, which sets standards for patents, trademarks, industrial designs, and copyrights.[a]

A selection of ISO data management standards:

- ISO/IEC 17789:2014. Cloud computing, Reference Architecture.
- ISO/IEC 19086-1:2016. Cloud Service Level Agreements.
- ISO 20022:2013. A standard for electronic data interchange between financial institutions.
- ISO/IEC 27001:2013. Specifies a management system for information security. This standard forms a basis for most ICT security certification programs.
- ISO/IEC 27018:2014. A standard, developed to provide appropriate technical and organizational measures to protect personal data.
- ISO/IEC 27017:2015. The current standard for cloud information security controls.
- ISO/IEC 27701:2019. An extension to ISO/IEC 27001/27002 for privacy information management.
- ISO/IEC 38500:2017. The series for governance of IT for an organization.

[a] World Intellectual Property Organization. About WIPO Standards.

Data Classification

To facilitate flexible data use policies while maintaining high standards of security, governments may elect to impose data classification frameworks to differentiate data according to security requirements. Classification would establish specific procedures on how high-security data are to be treated, reducing ambiguity in how such data are stored, transferred, or processed. Many initiatives have not been effective due to the lack of clarity on data classification and policies. As such, the security function of data classification enables it to be a foundational layer for data sharing.

Classification is often tiered, with each class necessitating a new baseline set of access and physical or information security protections appropriate to expected threats.[25] Commonly accepted international best practice attempts to minimize the number of tiers to reduce complications and the risk of misfiling.

Data classification establishes clear, harmonized standards for data security across government agencies. Many iterations of data classification may require that higher tiers of classified data are stored within data centers located in-country. However, caution should be exercised in ensuring that these storage requirements are applied selectively and with an awareness of the potential impact on cross-border data flows. Circumstances where such classification mandates have been too widely scoped have resulted in data localization, which has a potential chilling effect on foreign investment due to restrictions imposed on potential inbound investors. New and emerging global privacy laws, like the European Union's GDPR and the California Consumer Protection Act, give citizens the right to access, erase, and amend their personal data. Strong data classification policies allow organizations to verify their legitimacy and respond to requests in a manner consistent with the law in question. For example, the Government of the Republic of the Philippines has implemented an archetypical data classification framework that reflects sound international consensus on the issue (Box 6).

[25] Government of the United Kingdom, Cabinet Office. 2018. Government Security Classifications May 2018. United Kingdom.

Box 6: Data Classification Tiers in the Philippines

The Philippines' data classification framework is based on the international best practice of observing a minimal number of tiers and is illustrative of the concept of data classification more generally. The Philippines' data classification tiers are, from most to least sensitive: i) highly sensitive government data and above-sensitive government data, ii) sensitive government data, and iii) non-sensitive government data (Table).

Each tier is associated with specific storage requirements and guidelines. For example, highly sensitive government data, often associated with issues of national security or defense, must be stored on private clouds in on-site facilities or data centers on Philippine soil. Such data are subject to encryption requirements. In contrast, unclassified and publicly available non-sensitive data can be stored in an accredited public cloud, whether onshore or offshore.[a] The chart below illustrates the three tiers used in the Philippines' data classification framework.

Table: Three Tiers of Data Classification

Tier 1: Non-sensitive Data	Tier 2: Sensitive Data	Tier 3: Highly Sensitive or Above-Sensitive Data
Open, publicly available, and unclassified information	Restricted data such as financial and medical records	Classified information such as vital military and diplomatic information
Stored on accredited public cloud or the Philippine GovCloud	Stored on accredited public cloud or the Philippine GovCloud and has encryption requirements	Requires private and on-side cloud deployment, storage onshore, and has encryption requirements

[a] Government of the Republic of the Philippines, Department of Information and Communications Technology. 2020. Amendment to Department Circular No. 2017-002 Regarding Government's First Cloud Policy. Manila.

Data Protection Regulation

Governments across the world are taking note of the increasing importance of personal data protection regulations which empower government regulators to exert pressure on data controllers and processors to ensure that the rights and privacy of data subjects are respected and maintained. Such regulatory frameworks are fundamental to building public trust in the ability of state mechanisms to protect their data and play a significant role in the promotion of digital transformation at a societal level, including the expansion of digital government initiatives. As noted by the International Association of Privacy Professionals, data protection is not just about security but also the creation of policies which promote the fair use of personal data.[26]

Government action on this front has intensified over the past decade. A United Nations Conference on Trade and Development (UNCTAD) report on data protection shows that 57% of countries in the Asia and Pacific region have legislation on data privacy and protection, though not all are comparable.[27]

[26] International Association of Privacy Professionals. Data Protection.

[27] UNCTAD. Data Protection and Privacy Legislation Worldwide.

Many data protection regulations have emulated language and the general organizing framework of the European Union's GDPR, which codified many regulatory concepts associated with data protection.[28] Aspects of the GDPR that have become commonplace include core data rights such as data portability, and obligations including breach notification requirements under which data controllers are required to notify supervisory authorities and affected individuals if personal data has been breached.

As with other aspects of data governance, data protection regulations should be fit-for-purpose and assess any potential impact on cross-border data flows. Regulatory harmonization across different jurisdictions and regions on privacy issues can be an especially thorny issue due to methodological and ideological differences. Regional organizations can play a part in facilitating discussions and promoting shared principles, which can pave the way for firmer regulatory alignment between participating governments.

Organizations such as the Organisation for Economic Co-operation and Development (OECD), Asia-Pacific Economic Cooperation, and the Association of Southeast Asian Nations (ASEAN) have all produced baseline privacy principles or frameworks to aid in the development of regulations at the national level for member economies. Such principles can serve as useful foundations for national regulators and promote best practices (Table).

Table: Comparison of OECD, ASEAN, and APEC Privacy Principles

Principles that cover:	OECD Privacy Principles[a]	ASEAN Privacy Framework[b]	APEC Privacy Framework[c]
Collection, purpose of using data, and notification of personal data	• Collection Limitation Principle • Purpose Specification Principle • Openness Principle	• Consent, Notification, and Purpose • Retention	• Preventing Harm • Collection Limitation • Choice • Notice
Disclosure of personal data for purposes beyond the original purpose	• Use Limitation Principle	• Transfers to Another Country or Territory	• Uses of Personal Information
Accuracy and updated personal data	• Data Quality Principle	• Accuracy of Personal Data	• Integrity of Personal Information
Risks, loss or unauthorized access, destruction, modification of data, etc.	• Security Safeguards Principle	• Security Safeguards	• Security Safeguards
Ability of individuals to correct their personal data	• Individual Participation Principle	• Access and Correction	• Access and Correction
Accountability in terms of complying with the full principles	• Accountability Principle	• Accountability	• Accountability

APEC = Asia-Pacific Economic Cooperation, ASEAN = Association of Southeast Asian Nations, OECD = Organisation for Economic Co-operation and Development.

[a] OECD. 2013. *The OECD Privacy Framework*. Paris.
[b] ASEAN. 2012. *Framework on Personal Data Protection*. Jakarta.
[c] APEC. 2005. *APEC Privacy Framework*. Singapore.

Source: Authors.

[28] Intersoft Consulting. General Data Protection Regulation, European Union.

Cybersecurity

While the increasing breadth and quality of data held by governments is a strength that can be capitalized upon for good public outcomes, those same factors also make penetrating government systems an attractive opportunity for bad actors. This is especially the case given the increasingly interconnected nature of government systems, which can allow cyber attackers easy entry points into a wide variety of targets. Cyber incidents which result in the disclosure of large quantities of citizen data, or which inhibit access to citizen services or data, seriously damage public trust in government digital transformation initiatives and inhibit efforts to secure further stakeholder buy-in.

In the context of data management, cybersecurity refers to ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of data. Effective cybersecurity policies and frameworks are thus key to preventing, detecting, and mitigating cyber threats and risks. The ISO's ISO/IEC 27000 family of standards address information security management, with ISO/IEC 27001 being the best known and most widely adopted. Promoting adherence to guidelines and standards established within such international frameworks can serve as a strong starting point for governments seeking to ramp up security around potential threat surfaces. Governments may further seek to create their own assessment and diagnostic programs or certifications to determine information system security, though standards of assessment should, as ever, take reference from international best practices.

Government computer emergency response teams (CERT) play a significant role in helping mitigate the effects of cyber attacks on government data reservoirs. Such entities directly address risks associated with cyber threats across government agencies, monitoring for emergent threats while directly intervening when necessary to intercept attacks as they emerge and aid in recovery processes if attacks succeed. As government systems develop in complexity and connectedness, efforts can be made to expand the growth and scope of CERT entities, as well as building lines of communication with other government agencies to improve response times.

Some governments have sought to create or appoint separate agencies to handle the development of cybersecurity policy. Such cybersecurity agencies differ in role from CERTs in focusing more on cross-agency coordination, policy formulation, research, and advocacy or education. Such organizations can aid efforts to improve whole-of-government cyber readiness by developing activities that educate and inform stakeholders in government agencies about cyber threats, thus improving education and potentially reducing threat surfaces which might be used to illegally access public data.

Governments may also seek to develop formal cybersecurity legislation to ensure that crimes which specifically affect data and online spaces can be adequately addressed under their legal frameworks. Such legislation should pay due attention to data-related crimes and establish proportionate penalties and enforcement mechanisms.

The Japanese government's Ministry of Economy, Trade, and Industry; Ministry of Internal Affairs and Communications; and the National Centre of Incident Readiness and Strategy for Cybersecurity jointly operate the Information System Security Management and Assessment Program (ISMAP).[29]

[29] Information System Security Management and Assessment Program. https://www.ismap.go.jp/csm.

Based on the US government's Federal Risk and Authorization Management Program, ISMAP is a government-provided security assessment, authorization, and monitoring initiative targeting cloud service providers (Box 7).

Box 7: Ensuring Information Security on the Cloud with the Information System Security Management and Assessment Program

The Information System Security Management and Assessment Program (ISMAP) seeks to establish a common set of security standards for cloud service providers (CSP). While assent to ISMAP is not required for CSPs seeking to operate in Japan for private sector clients, approval under the program is strongly encouraged for CSPs which intend to participate in government procurement and handle public sector data. Successful approval and registration under ISMAP allows CSPs to have their bids and tenders more smoothly and quickly approved by government agencies.

ISMAP was introduced in June 2020 to facilitate the more rapid introduction of cloud services into the Japanese public sector while ensuring that all participating CSPs observed a baseline standard of information security management. ISMAP also ensures that all CSPs seeking to participate in Japanese government tenders comply with Japan's information security agenda, potentially positioning it in a leadership role vis-à-vis policy formulation.

Data Life Cycle

The need to consider the life cycle of data is an increasingly vital, if often overlooked aspect of data management policies. Considering data life cycles requires a holistic understanding of how the data are to be acquired, what it is to be acquired for, how it is to be used for its intended purpose, whether it can be re-used, and how it is ultimately disposed of or archived.

Life cycle considerations are a key aspect of adherence to the ISO/IEC 27001 standard, which is a widely adopted and authoritative standard providing guidance to organizations on establishing, maintaining, and improving information security management systems. To be certified under the standard, organizations must adopt a life cycle approach to security. Under such an approach, the management of system and data security follows a cyclical and continuous process of protection and improvement, beginning from implementation until the system or data are deleted.[30]

The architecture and processes used within a data life cycle may change according to the demands of data users and the nature and purpose of the data. Variable factors include volume, type and range of data, speed and rate required in accessing the data, variability in characteristics of the data, and trustworthiness of the data.[31]

Given the sensitivity of data collected and held by governments, both in terms of citizen privacy and implications for national security, developing a strong understanding of how data are used, and when

[30] ISO. Information Technology—Security Techniques—Information Security Management Systems—Requirements.

[31] ISO. 2015. ISO/IEC JTC 1, *Information technology Big Data Preliminary Report*. Switzerland.

it is to be securely disposed of or stored, is likely to grow in importance. Governments may seek to implement policies on data retention, including archiving and data destruction. Data storage has become cheaper over time, but costs to build database infrastructure to search, restore, and access data remain high, and there is a risk of loss of access caused by malicious actors. Data protection laws can include guidance on data life cycles, but there are more bespoke tools which address this issue.

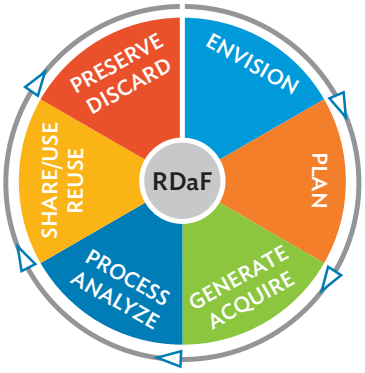
Some government organizations have developed frameworks to address the issue of data life cycles, though implementation is often limited. One such example is the US government's National Institute of Standards and Technology Research Data Framework (Box 8).

Box 8: Mapping the Life Cycles of Research Data in the United States

The National Institute of Standards and Technology (NIST), a United States government organization which oversees the issuance and maintenance of technological standards, has developed a model which maps stages of the life cycle of data used for research. The NIST Research Data Framework identifies and describes the following stages in the life cycle of data:

- **Envision:** The overall strategies and drivers for collecting data are reviewed.
- **Plan:** The organization maps how to manage the data throughout the life cycle.
- **Generate/acquire:** Raw data are generated, acquired, and collected.
- **Process/analyze:** The organization acts on the data to make it useful.
- **Share/use/reuse:** The data are used or shared to achieve the purpose for which the data was collected.
- **Preserve/discard:** The purpose of the data have been fulfilled and the data are deleted or kept as records.

Research Data Framework Data Life Cycle



RDaF = research data framework.

Source: NIST. 2022. *Research Data Framework (RDaF)*.

Cultural Issues

For many governments, the transition to more data-based governance models and the increased data management methodologies those models entail is not an easy one. Hardened aspects of organizational culture can be particularly persistent impediments to more agile decision-making and policy implementation. Creating a "data culture," where the use of data becomes a norm among employees and leaders in the organization as well as citizens, can improve organizational cohesion on data management issues, and drive positive outcomes in internal and external organizational processes.[32] This process of developing a data culture needs to start early.

> "Culture is how things are done, and so it can block or drive the adoption of data-driven services. Understanding the interaction of multiple factors to create better digital experiences with government is essential, starting with exploring the impact on staff, leaders, and customers."
>
> ***Jane Treadwell***
> *Lead, Government Transformation, Amazon Web Services*

In cases of discomfort or concerns over widespread use of data in the organization, organizations must demonstrate leadership regarding data issues at the highest level to reassure employees.[33] Leaders play a key role in ensuring the successful adoption of a data-driven culture and should communicate the benefits that data are bringing to the organization and employees and demonstrate that ethical concerns are considered and managed.[34] Similarly, any concerns that citizens have on data privacy and security should be addressed by their representatives.

In addition, organization leaders should also demonstrate the usefulness of data by using data to make decisions, even if the data are contrary to their beliefs (footnote 33). Data should be treated as an asset, and efforts should be made to demolish data silos within the organization to ensure that teams share data and work collaboratively to make use of it.

Singapore, for example, has adopted a two-pronged approach to developing a data-driven culture within its public sector. From the bottom up, agencies that aspired to be leaders in driving Singapore's Government Data Strategy were cultivated as champion agencies and given opportunities to build partnerships with other agencies.[35] From these collaborations, champion agencies then shared knowledge and best practices through workshops and on online collaborative platforms such as Data Professionals@Workplace. These efforts helped build a larger data community among government employees and establish a stronger data culture across the government (Box 9).

---

[32] D. Waller. 2020. 10 Steps to Creating a Data-Driven Culture. *Harvard Business Review*. 6 February.

[33] I. Vachhrajani. 2019. How to Create a Data-Driven Culture. *Amazon Web Services*. 9 September.

[34] L. Goasduff. 2019. Create a Data-Driven Culture by Influencing 3 Areas. *Gartner*. 14 November.

[35] Interview with Kelvin Goh, deputy director at GovTech and SNDGO, 11 January 2022.

Box 9: Building a Data Culture in Singapore

Singapore's government technology agency (GovTech) also organizes several initiatives to continue promoting data-driven approaches and attitudes. It convenes an annual visual analytics competition called the Data Arcade Tournament to encourage Singapore public service officers to upskill their data capabilities and adopt data-driven approaches to their work. GovTech has also established a competency framework and training road map that recommends suitable courses that officers can take to improve their digital and data competencies, depending on their job role.

The Singapore government has appointed a chief digital strategy officer in every ministry to oversee the delivery of their ministry's Digital Government Blueprint targets and digitalization plans. This includes driving the agency's data transformation strategy and initiatives.

Multilateral Initiatives

Governments are ultimately responsible for developing data management policies relevant to their specific contexts and addressing issues they may uniquely face. However, engagement with multilateral initiatives which promote productive data management principles can be a useful means of becoming exposed to international best practices and facilitating transnational regulatory alignment in the interests of enabling cross-border data flows.

The growing popularity of digital trade agreements also presents a new avenue for convergence on data issues, with many such agreements integrating language which explicitly supports continued promotion of uninhibited free flows of data across borders (Box 10).

Box 10: The Role of Asia-Pacific Economic Cooperation Cross-Border Privacy Rules in Facilitating Cross-Border Data Transfers

Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) is an example of a multilateral accountability mechanism for data transfers with substantial regional outreach. Currently, the CBPR has been adopted by nine member economies (Australia; Canada; Japan; Mexico, the Philippines; the Republic of Korea; Singapore; Taipei,China; and the United States [US]).a The CBPR is recognized within several trade agreements as a valid mechanism facilitating cross-border data transfers. The United States–Mexico–Canada Agreement and the US–Japan Digital Trade Agreement ensure that participating companies can reference compliance with the CBPR as a shared basis for data transfers.b

[a] APEC. 2021. *Data Protection in the Asia and the Pacific Region and Cross-Border Privacy Rules*. Singapore.

[b] Government of the United States, Office of the United States Trade Representative. 2019. *Fact sheet on US-Japan digital trade agreement*. Washington, DC.

There are tangible benefits to be had from having a strong data governance framework. For example, in the Netherlands, census data are taken entirely from existing databases which results in a 99% cost reduction.[36] Countries like Portugal, the Republic of Korea, and the UK developed dashboards to track the COVID-19 pandemic, and this was largely possible due to strides already taken in their national data strategy (footnote 36).

Takeaways

A sound data governance framework should be in line with a country's values and principles and should be a powerful engine for growth for its citizens and economy. The principles and examples outlined in this section offer a reference and inform policy makers on existing frameworks so they need not start from scratch. These include developing sound and implementable policies to ensure data can be managed and used appropriately such as:

- Government data storage regulations
- Data classifications
- Data protection regulations
- Cybersecurity
- Data life cycle

Apart from the data policies and regulations that governments can develop, each country would still face unique challenges. Crafting the right mindset is equally if not more important, while there are also influencing factors which emerge from beyond borders as well. These are covered under culture and multilateral initiatives.

These guidelines help to ensure that governments know what data they have, where it is, and what it contains. Ultimately, the goal is to have an interoperable and connected government data ecosystem which can improve administrative efficiency, citizen experience, and innovation.

Identifying Quick Wins

Rationalizing investments in data management can be challenging given the scale of institutional transformation that often becomes necessary. Securing long-term stakeholder buy-in is thus an immediate priority when designing a data management strategy. This will often entail targeting quick wins or initiatives that can succinctly embody the value of data management reforms to government agencies and citizens. Such initiatives are often exercises in communication, which help to illustrate the benefits that can result from concerted engagement with, and investment in data management.

An emerging trend in government digitalization is the increasing adoption of public sector technology stacks, or GovStacks. GovStacks are collections of diverse digital products, solutions, and frameworks assembled to constitute a shared resource which can be used across government agencies. This allows different agencies to develop and deploy new services rapidly (Box 11).

[36] Nationaler Normenkontrollrat. 2017. *Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren (More performance for citizens and companies: digitize administration, modernize registers)*. Germany.

Box 11: Building Digital Infrastructure with Government Technology Stacks—A Novel Enabler of Government Digitalization

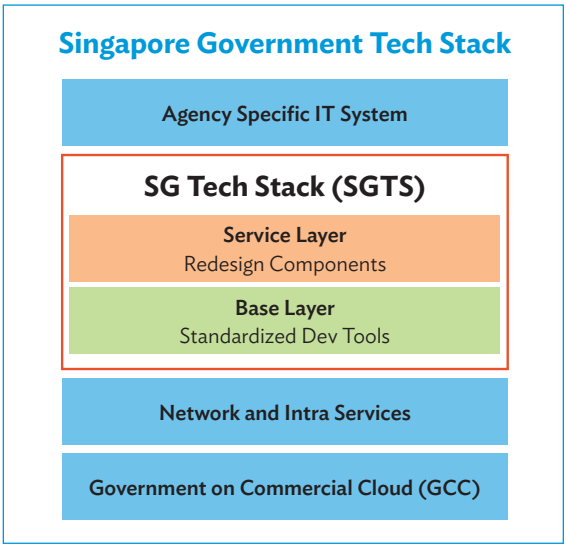
The intent of government technology stacks or GovStacks is to facilitate a degree of centralized curation to ensure the quality and security of applications integrated into government digital infrastructure and thereby secure software supply chains, as well as lowering implementation costs by enabling code reuse across different agencies and guaranteeing interoperability.

GovStacks allow for the centralized development, selection, and dissemination of pre-selected technologies for use across the entirety of a government's supply chain. This allows for agencies across government to quickly adopt new digital solutions in a sustainably scalable manner. Many of the digital solutions contained in a GovStack are likely intended to facilitate data analysis and collection. This, in turn, equips government agencies with the tools to more efficiently take advantage of data resources they might have immediate access to, or which they might be able to gain access to.

In India, a GovStack initiative was established through IndiaStack, an ambitious project of creating a unified software platform to bring India's population into the digital age. IndiaStack is essentially a combination of the National Payment Corporation of India's project with Aadhaar's identity and authentication expertise that are accessible through application programming interfaces (API). Through APIs, IndiaStack aims to unlock data and payments at population scale. IndiaStack has enabled 67 billion digital identity verifications and ₹5.47 trillion in monthly mobile payments.

Another example is the GovStack initiative, which is a multi-stakeholder initiative led by the Federal Ministry for Economic Cooperation and Development, Gesellschaft für Internationale Zusammenarbeit, Estonia, the International Telecommunication Union (ITU), and the Digital Impact Alliance. GovStack aims to accelerate the digitalization of government services through a set of digital building blocks that allow national public agencies to harness the power of technologies. Using GovStack technology, the ITU has helped several countries establish circular economies through a systems approach in which producers contribute to device recycling and reuse.

The Government of Singapore is operating a Singapore Government Tech Stack (SGTS) to facilitate the use of platform tools at a whole-of-government level along a two-layer architecture. At the services Layer, the SGTS facilitates the adoption of digital services in the areas of data analytics, data science, data transfer, system design, digital identity, and the Internet of Things across all government agencies. At the base layer, the SGTS provides tools related to application design, covering areas such as communications, toolchain, runtime, monitoring, and service management.



As in the figure indicates, the SGTS is intended to sit just below agency-specific IT systems as a shared standard of design components and development tools that ensures that individual agencies are running interoperable systems and settings, while still allowing agencies flexibility to expand their approaches and tool kits beyond the SGTS if needed. Many tools and application programming interfaces packaged within the SGTS are developed internally by the Singapore government technology agency (GovTech) or constitute stacks which are themselves assembled by GovTech.

Source: Singapore Government Developer Portal. 2022. *Singapore Government Tech Stack*.

Identifying Use-Cases

Even though data have become a common element of daily life, its enormous impact remains in many ways invisible to ordinary citizens and government officials. Clearly illustrating use-cases for data that reflect the scale of its effect on daily life can be an important step to securing stakeholder buy-in. This can aid in promoting a clearer understanding of how data management can affect the operation and efficiency of public programs. Proceeding from a use-case-first perspective also ensures that real-life problems are accurately identified and solved, allowing investigating authorities to create optimized implementation strategies for areas of improvement or development. Identifying use-cases also offers the possibility of building standardized components across a range of applications which will make scaling up easier down the line.

Singapore is an example of a government which approached the challenge of data management by first seeking to determine use-cases for data management practices (Box 12).

Box 12: Singapore's Focus on Use-Cases

The Government of Singapore formed a Government Analytics Team in 2014, which focused on identifying use-cases that could serve as proofs of concept for further investments into data management.[a] This team would integrate high-level data engineering capabilities and transition into the Data Science and Artificial Intelligence Division (DSAID) at the Government Technology Agency.

DSAID would later collaborate with the Data Strategy and Exploitation team, which was strongly focused on policy issues, to identify gaps in Singapore's data architecture. This led to the development of the Singapore Government Digital Strategy (GDS), which was incorporated into the Digital Government Blueprint in 2018.[b] The GDS established a Government Data Office to i mplement key data management reforms across four dimensions: architecture, infrastructure, education, and use-cases.

> "Agencies have to be able to see quick wins to decide to invest further in data transformation and to reap deeper benefits of modernizing their data processes, infrastructure, and culture. For example, when agencies are able to see first-hand how helpful it is to easily access cross-agency data while maintaining strong data protection, they are more open to exploring other aspects of data transformation, including the use of data analytics and machine learning, and investing in human resources and capabilities in this area."
>
> ***Kelvin Goh***
> *Deputy Director at GovTech / Smart Nation and Digital Government Office Singapore*

[a] D. Mao. 2019. Bringing Data into the Heart of Digital Government. *Civil Service College*. 8 August.
[b] Smart Nation Singapore. 2018. *Digital Government Blueprint*.

Establish Innovation Sandboxes

Securing buy-in from the private sector can have a ripple effect on efforts to broaden the uptake of good data management practices. The attractiveness of large-scale public sector procurement contracts can serve as a strong incentive for digital service providers to adhere to data management requirements established by government. In addition, the introduction of regulatory sandboxes to incentivize domestic innovation and entrepreneurship and promote foreign investment can lead to the organic development of a thriving data-based ecosystem. A sandbox is a regulatory approach that allows live, time-bound testing of innovations under a regulator's supervision.[37]

The existence of such an ecosystem can be a powerful incentive for further investment, leading to a virtuous cycle of data-oriented value creation. Sandboxes can thus generate enthusiasm for digital innovation in the short term, while resulting in stronger and more holistic regulatory approaches in the long term. While regulatory sandboxes level the playing field for small businesses and are consumer-centric, it can be challenging to sustain short-term successes. Even though it requires substantial effort and time, laying the groundwork for an innovation culture can lead to a more effective and efficient public sector.

Several countries in the region have already established regulatory sandboxes, including Japan, which introduced its approach to promote the development of innovative technologies and business models across a variety of sectors, including health care, mobility, financial services, and transportation (Box 13).

Box 13: Japan Uses Sandboxes to Develop Agile Regulations

The Government of Japan introduced a 'sandbox framework' policy in 2018. Under this policy, both domestic and foreign companies, which ordinarily are unable to operate in Japan due to regulatory restrictions, can apply to conduct a demonstration of their technology or service to test new technologies.[a]

These demonstrations are closely monitored for effectiveness and social or economic impact, and data are gathered for analysis by government, with the aim of establishing how the technology interacts with existing regulations and if changes need to be made to facilitate their development.

Using the sandbox framework allows governments to collect data and leverage data-driven policies and regulations. For example, the city of Fukuoka was declared a national strategic special zone for e-scooter use, and sandbox regulations were put in place to allow for their use across the municipality. This allowed the government to collect data on the use of electric scooters and evaluate their effects on traffic congestion and determine if they could alleviate chronic parking issues.[a] This also allowed leaders at the municipal and national level to gather valuable data on accident rates, and whether the use of such devices could constitute a risk to public safety.

Private sector advocates for deregulated e-scooter use also supported the policy as an outstanding opportunity to generate and gather data to make the case for formalized business and user-friendly regulations on e-scooter use.

[a] Sponsor Content from the Government of Japan. 2020. How the Japanese Government's New 'Sandbox' Program Is Testing Innovations in Mobility and Technology. *Harvard Business Review*. 11 February.

[37] UN Secretary General's Special Advocate for Inclusive Finance for Development. 2020. *Briefing on Regulatory Sandboxes*.

The use of sandboxes allows the Japanese government to explore more novel uses of data in a closely controlled environment, allows a regulator to oversee and evaluate the potential use of the new services, and ensures risks are identified before the product or service is commercialized.

Generate Ideas through Public Contests

Increasing awareness of the importance of data issues among expert communities and the public can go hand-in-hand with developing new and innovative data-based digital solutions. An especially effective means of building public awareness of government investment and engagement on data issues is through organizing public contests for mobile applications or data use-cases. This allows government to build awareness, while crowdsourcing digital solutions and identifying skilled talent which can be attracted to government projects.

One example comes from Kazakhstan, which was the first country in Central Asia to spearhead an Open Government initiative in 2007 (Box 14).

Box 14: Kazakhstan's Contest to Build Apps Using Government Open Data

Following the commencement of its Open Government initiative in 2007, the eGov Portal was subsequently launched in 2012. Thereafter, the state program Digital Kazakhstan was adopted in late 2017, leading to the development of 17 initiatives and over 120 events.[a]

Shortly after the introduction of the eGov Portal, Kazakhstan ran a competition among national universities and colleges for mobile application development based on a beta version of the country's Open Data platform in 2014.[b] The objective of the contests was to build the Open Data platform's functionalities, as articulated in the Information Kazakhstan 2020 state program.

The winning team developed a catalog of kindergartens in the capital Astana to show their locations and contact details on an online map. Other submissions included an application that allows users to view individuals and entities with various publicly available electronic licenses.

[a] Digital Kazakhstan.
[b] A. Kaulanova. 2014. The Rise of Open Data in Kazakhstan. *World Bank Blogs*. 8 December.

Takeaways

Governments are experimenting with diverse and creative ways to drive transformation and get stakeholder buy-in. The three general approaches are:

- Identifying use-cases
- Establishing innovation sandboxes
- Generating ideas through public contests

These approaches provide useful tips on kickstarting data management and transformation in various contexts.

There is no one-size-fits-all approach, and it is up to governments to decide which is the right one or a combination of approaches that aligns with their national data strategy. Underpinning all these efforts should be the right infrastructure and a long-term vision on how to translate it into sustained digital transformation.

Scale Up the Use of Data

With stakeholder support secured, government agencies are likely to be better positioned to expand the scope of data-driven public sector activities to actualize medium-term benefits. This necessitates the development of institutional infrastructure, including digital transformation agencies which can harness data-driven efficiencies to build bespoke digital solutions, and data architecture to facilitate direct access to data reservoirs from different agencies. Appropriate attention should be committed to capacity-building exercises within government to ensure that civil servants are appropriately equipped to aid in the upscaling of data-driven digital solutions within and across government agencies.

Establish a Dedicated Digital Agency

The creation or designation of an agency to coordinate the development and dissemination of data management priorities is a vital step, which is often tied to the release of an initial strategic vision. In many cases, a national action plan on digital transformation or data management may elect to either create or designate a digital agency to manage a whole-of-government digital transformation. For instance, Thailand's Digital Government Development Authority is a designated lead agency tasked to drive the public sector's digital transformation efforts. Action plans which are more explicitly tailored to address data management issues may either build on appointments made under existing digital transformation plans, or create entirely new entities, depending on the political circumstances and specific needs of the government in question.

There are advantages and disadvantages in designating an agency or creating one planned to address data management. Designating an existing agency may allow the data management agenda to benefit from existing institutional mechanisms, resources, and leverage, but may also result in more conservative approaches constrained by hardened bureaucratic practices or a less-than-clear overall institutional mandate. In contrast, creating a new agency may result in an entity possessing clarity of purpose and expertise, and a willingness to push boundaries to achieve success, but also one which lacks institutional legitimacy or sufficient political leverage to pursue its agenda.

Regardless of whether an agency is created or designated, carefully delineating its responsibilities, authority, and powers relative to other similar agencies at an early stage is of vital importance. Failing to do so may result in responsibilities and funding being split among multiple agencies, which could inhibit the design and deployment of a single coherent data management agenda and lead to wasted resources as a result of duplicated effort.

A core component of this process will involve deciding how individual agencies will interact with the data management agency, including whether the agency will coordinate data management processes directly, through attached departmental staff, via internally appointed liaison divisions, or through some other means.

Building an agency with an explicit mandate to oversee and coordinate data management issues can be a make-or-break decision that can either supercharge or hamper a government's data management and wider digital transformation agenda. The decision and commitment toward establishing such an agency should never be seen as "too late," with both developed and emerging economies known to face similar challenges. Thailand is one of the countries that transformed an existing agency to spearhead its digital transformation (Box 15).

Box 15: Driving Government Transformation through Thailand's Digital Government Development Agency

The Digital Government Development Agency (DGA) was established in 2018, replacing the former Electronic Government Agency under Royal Decree B.E. 2561. The DGA serves as a central agency for the digital government system to provide services and support for all government agencies related to digital government transformation. This includes creating digital services and integrating the government's data with security in place and upgrading digital skills among government personnel to support digital government operations.

In the same vein, the DGA takes the lead in data management practices, which include acceleration of the Thailand Government Information Exchange and the Government Data Exchange. The Government Information Exchange serves as a central database of government agencies designed to reduce the documentation burden on the private sector, improve efficiency by eliminating redundancy, and promote the use of digital IDs, including digital signatures among government agencies.[a]

The DGA is also accelerating development of the Government Data Exchange to create an integrated platform of government databases over the next 2 years by standardizing data exchange guidelines among government agencies.

[a] SEA_VET.net. 2021. Thailand's Digital Transformation Help to Boost Data Industry. 17 July. https://sea-vet.net/news/940-thailand-s-digital-transformation-help-to-boost-data-industry.

Data Architecture

When attempting to scale up data use, a foundational policy objective should be the definition and adoption of a coherent and implementable data architecture. The Open Group Architecture Framework defines data architecture as comprising models, policies, rules, or standards that govern which data are collected, and how it is stored, arranged, integrated, and put to use in data systems and organizations.[38] The Data Management Association's Data Management Book of Knowledge expands on this definition, noting that a data architecture defines the blueprint for managing data assets in line with organizational strategy, with strategic data requirements and templates and frameworks in mind.[39]

Data architecture is foundational because it informs how governments move forward with their data management agendas, and acts as a singular point of reference for all agencies to rely on in designing bespoke approaches in accordance with their specific needs. By establishing standard parameters for

[38] The Open Group, TOGAF Standard. Phase C: Information Systems Architectures—Application Architecture.

[39] Dama International. 2017. *Data Management Body of Knowledge 2*.

data management, data architectures help to mitigate deviation from core data management principles, while also allowing individual agencies to more clearly understand where and how they can build on established structures.

The establishment of a government-wide data management agenda without a well-defined and agreed-upon data architecture at a whole-of-government level risks radical misalignments in agency policy making. Such misalignments could result in the adoption of data principles which may be functionally incompatible with broader government approaches, or simply unaligned with international best practices. This could create system incompatibility issues in the long term, which may require significant investments in capital and human resources to rectify.

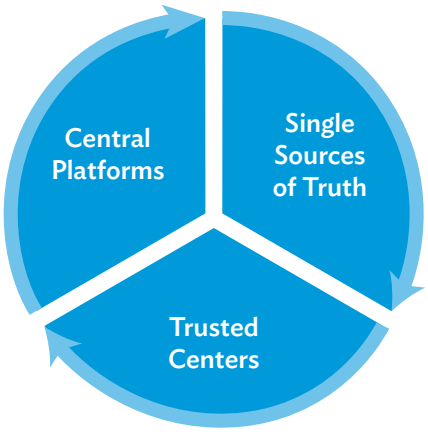
To avoid such misalignments, the Government of Singapore introduced a Government Data Architecture in October 2019 to promote the secure use and sharing of data across the public sector (Box 16).

Box 16: Sharing Clean and Authoritative Data Sets Using a Government Data Architecture in Singapore

Singapore's Government Data Architecture (GDA)revolves around the concept of core data, that is, data which is most frequently used by multiple public agencies. The GDA aims to facilitate sharing clean and authoritative data sets composed of core data in three ways.[a]

First, the GDA seeks to designate and build "Single Sources of Truth," which acquire, clean, and maintain high-quality core data. This core data are then fused and distributed to Trusted Centers. Fused core data sets are subsequently stored in Central Platforms including the Smart Nation and Digital Government Office Vault for data users to request, download, and analyze when needed. The GDA thus oversees the generation, collation, storage, and dissemination of core data across the Singapore government.

Singapore's Government Data Architecture



Source: Author's elaboration.

The GDA is intended to bypass existing bureaucratic inefficiencies associated with data sharing, which in the past has meant that responding to legitimate data requests could take between 6 and 13 months.[b] The centralization of data generation and storage means that public agencies can more freely delete unneeded data as required without being concerned that the data sets will no longer be available, thus reducing storage requirements and cutting down on digital clutter. The GDA also promotes secure data sharing, by ensuring that data security safeguards are standardized across all government data access points.

continued on next page

Box 16 *continued*

Plans are in place to leverage benefits brought about by the GDA directly. Singapore's Ministry of Trade and Industry has indicated that it will use GDA data to support its National Economic Research and Visualization Engine, while the Government Technology Agency will use GDA data to support the development of a platform for detecting grant fraud.

[a] Challenge. Ask A pro: Using Data Securely.
[b] Data.govt.nz. Government Data Strategy and Roadmap 2021.

Open Government Data

An increasingly vital component of government data management is open government data. This refers to initiatives which seek to make data reservoirs more widely available to the public. Open data access has the capacity to generate enormous social and economic benefits. According to an OECD analysis, data access and sharing is estimated to generate social and economic benefits worth between 0.1% and 1.5% of GDP annually, in the case of public sector data.[40]

Broadening access to public sector data can also function to offset the disproportionate market power of major tech firms, which are able to benefit from access to large proprietary data reservoirs. This enables smaller domestic firms to develop more competitive digital products and services, while also lowering barriers to entry for data-oriented foreign businesses to tailor service offerings to smaller markets. Improving the accessibility of government data can also have significant effects on civil society participation and generate positive social outcomes. The ultimate aim of open government is to encourage deep collaborations and thereby drive innovation. For such deep change and performance improvements to occur, there is a need to go beyond tools to a comprehensive, focused, and flexible change management process. Technology and policy are linchpins to the success of open government, and so are people. In making data more accessible, it is also necessary that critical areas like employee and citizen readiness are assessed and effective communication channels are in place. Improving the transparency of government operations can also lead to the development of a positive feedback loop where incremental improvements can emerge from input received from the public. Transparency can also inspire greater trust in government processes and lead to more participatory forms of civil–government collaboration.

Instead of simply seeking to publish as widely as possible to facilitate these possibilities, however, governments should ensure that open data reservoirs contain useful, trustworthy, and workable data. Open government data initiatives may thus involve making government-held data available, sourcing useful private reservoirs of data, and facilitating efforts to standardize them for usability before broadening access to them through public–private partnerships.

[40] OECD. 2019. *Enhancing Access to and Sharing of Data*. Paris.

Open government fundamentally changes the way citizens interact with their governments and can improve decision-making, help anticipate and better respond to risks, reduce costs, and enhance innovation. This requires worthy goals and well-designed processes along with an understanding of cultural contexts and the unique hurdles they generate.

A joint effort in Hong Kong, China between transport operators, a local university, and government agencies helped unlock actionable insights through a coordinated approach toward sharing data (Box 17).

Box 17: Promoting Intermodal Transport Data Sharing in Hong Kong, China Using a Data Trust

In 2018, the Government of Hong Kong, China expressed concerns regarding the lack of adequate data-sharing mechanisms relating to the jurisdiction's public transport services. This prompted the Transport and Housing Bureau to develop and promote data sharing between transport service providers, including the island's bus, ferry, tram, and metro service operators. Issues emerged when service providers expressed an unwillingness to cooperate due to concerns that their competitive advantages would be undermined by their participation in the initiative.

A data trust was established with funding from the government's Innovation and Technology Fund and developed using cloud resources provided by Hong Kong University.[a] This data trust was intended to function as an intermediary which would provide transport operators with relevant assurances related to commercial protections, logistical benefits, and user agnosticism to encourage their participation. The data trust was also required by transport operators to observe rigorous data security requirements to avoid potential liability issues.

Using data flows provided by transport operators, the data trust was used to create visualizations to examine a variety of use-cases. These included bus passenger routes, vehicle timings, and passenger numbers. Work is ongoing to integrate visualizations for newly submitted data from metro service providers and geolocation data corresponding to the location of major population and traffic centers.

In broadening access to data in an accessible and understandable format, the data trust initiative has allowed private sector operators a wider view of Hong Kong, China's overall transport ecosystem, and given government agencies an invaluable resource for urban and transport planning. Members of the public have also been able to more efficiently access information about high traffic regions and monitor transport patterns.

[a] Hong Kong University. 2021. *Intermodal Transport Data-Sharing Programme Final Report*. Hong Kong, China.

Data Marketplaces

A growing awareness of the value of data as a commodity has led to a bustling trade in data, especially with the growing demand for data due to emergent data-driven technologies such as artificial intelligence. Private sector data vendors have profited significantly from the expansion of this industry, and major data marketplaces have emerged to facilitate this growing economic sector, which is dominated by major data-holding organizations such as Google, and dedicated data-brokering businesses like Equinix or Snowflake.

Data marketplaces or data exchanges are a new concept currently being discussed by governments and nongovernment organizations such as the World Economic Forum.[41] As a concept, data marketplaces offer secure data sharing and enable open data to be re-used to create new solutions and innovations. These marketplaces address the underlying issue of information asymmetry and help to cultivate trust by using rules, enforcement mechanisms, transparency procedures, and other governance mechanisms.[42] With appropriate systems and processes in place, participants are more likely to leverage the data marketplace and bring together larger and more diverse data sets and sources to promote value creation (Box 18).

Box 18: India's Real-Time Data Marketplaces

India is exploring real-time data marketplaces. The National Institution for Transforming India (NITI Aayog) and the Centre for the Fourth Industrial Revolution India have developed a framework in consultation with a multi-stakeholder community to promote data exchanges with open, scalable architectures, and transparent and equitable governance models supported by sound incentivization principles.[a]

[a] World Economic Forum. 2021. *Towards a Data Economy: An Enabling Framework*. Cologny.

Governments may seek to promote access to these data marketplaces for domestic companies, and potentially develop their own mechanisms to help bridge the gap. As discussed earlier, open data solutions are a viable means of equalizing access to government-held data. However, governments may be able to exert greater control over standards development, policy making, and rules formulation in relation to the data industry if they can take a more active approach to data marketplace formation and centralization.

Playing an active role in the trade of data can have significant effects on the accessibility of data for domestic industries and less well-resourced market participants. Directly participating in the development of data markets could also help ensure that data subjects are appropriately compensated for the use of their data in commercial products or services.

[41] World Economic Forum. 2021. *Data-driven Economies: Foundations for Our Common Future*. Cologny.

[42] World Economic Forum. 2021. *Developing a Responsible and Well-Designed Governance Structure for Data Marketplaces*. Cologny.

The development of such initiatives is best undertaken in collaboration and with the cooperation of major data holders and providers to ensure the greatest possible industry buy-in and allow for clear lines of communication between governments and industry stakeholders.

Proactively promoting data marketplace development would strongly signal an interest in engaging with the private sector and providing regulatory support to the data economy. Approaches that too strongly signal support for data sovereignty or similarly restrictive approaches to data management may deter potential investment and diminish the ability of local digital service providers to expand regionally.

An innovative example comes from Japan where the government has been working with third-party information banks which have been certified by the government to collect personal data and use a consent management system to allow the bank to share the data with third parties based on the consent conditions agreed on by the data subjects (Box 19).

Box 19: Building Business Confidence with Japan's Information Banks

Seeking to promote wider accessibility of personal data to Japanese companies, Japan's Ministry of Internal Affairs and Communications developed a project with the town of Misono in Saitama Province to develop and promote an information bank.[a] This will collate voluntarily provided citizen information from different businesses and store it in a central location before making it available to third-party data-using organizations at a fee. Individuals who opted to contribute information would be duly compensated for their data.

A data trust was established with funding from the Government of Hong Kong, China's Innovation and Technology Fund and developed using cloud resources provided by Hong Kong University.[a] This data trust was intended to function as an intermediary which would provide transport operators with relevant assurances related to commercial protections, logistical benefits, and user agnosticism to encourage their participation. The data trust was also required by transport operators to observe rigorous data security requirements to avoid potential liability issues.

Under this scheme, Japanese retail giant Aeon, insurance provider SOMPO Himawari Life, pharmaceutical retailer Welcia Pharmacy, and lifestyle health-care provider Japan Healthcare provided a variety of personal data, including credit purchase information, health examination results, and lifestyle data. Each data provider benefited from the data provided by other providers. Participating companies consequently analyzed the acquired data to provide bespoke recommendations for participating individuals. These included personalized health and wellness recommendations as well as targeted insurance advice.

It was noted, however, that even when provided with data, many participating businesses did not have clear ideas about how to process and analyze it to effectively provide novel recommendations. The project concluded that while initial results were promising, there was definite scope for the scheme to be expanded to advise data purchasers on how they might make use of the data and how it might align with existing data sources.

[a] Government of Japan, Ministry of Internal Affairs and Communications. Information trust function utilization promotion business: Demonstration project casebook.

Working with Vendors

Galvanizing public–private partnerships can be an especially vital means of securing access to valuable data sources. While governments have access to a wide array of data, many private companies have more selectively curated data reservoirs due to their specific needs and use-cases. While narrower in their scope, analysis of these data reservoirs is likely to result in positive outcomes for the development of public services as well. Governments across Asia have expressed interest in directly collaborating with large data-holding companies to maximize access to data resources.[43]

For example, the ride-hailing and food delivery company Grab partnered with regional governments in the Asia and Pacific region to share data and provide insights on how to improve traffic flows. Grab's large data reservoirs are especially well suited to providing guidance on these issues, due to the company's strong focus on issues such as routing optimization and traffic management (Box 20).

Box 20: Working with Grab on Smart City Traffic Optimization in the Philippines

An initiative launched in 2016 involved Grab, the World Bank, and the Philippine government aimed to improve traffic flow in major metropolitan areas such as Cebu and Metro Manila, which have historically suffered from high levels of traffic congestion.[a] Anonymized driver GPS data provided by Grab was used to jointly develop free, open-source tools which provide traffic statistics, including vehicle speed, traffic flows, and intersection delays. Two such tools are OpenTraffic, which facilitates the analysis of traffic speed and flows, and DRIVER, which can identify road incidents and improve emergency response timing.

In addition, the initiative has enabled city governments to collect and process more data, increasing the potential for smarter solutions.[b] The Government of the Philippines worked with other ride-sharing companies to further develop this initiative, to unlock efficiencies for transport regulators and associated government organizations. These initiatives have produced data-driven improvements including refinements to traffic signal timing along the primary west–east arterial road in Cebu City, and a drop in transportation costs for commuters.[b]

The successful operationalization of OpenTraffic and DRIVER in the Philippines has created the groundwork for its expansion to other countries in the region, such as Malaysia.

[a] Grab. Philippines: Real-Time Data Helps Philippine Government Improve Traffic Management in Major Cities.
[b] S. Debere. 2016. Open Traffic Data to Revolutionize Transport. *World Bank*. 19 December.
[c] Grab. Grab and MDEC Together with the World Bank Group Launch OpenTraffic Platform in Malaysia to Combat Local Traffic Woes.

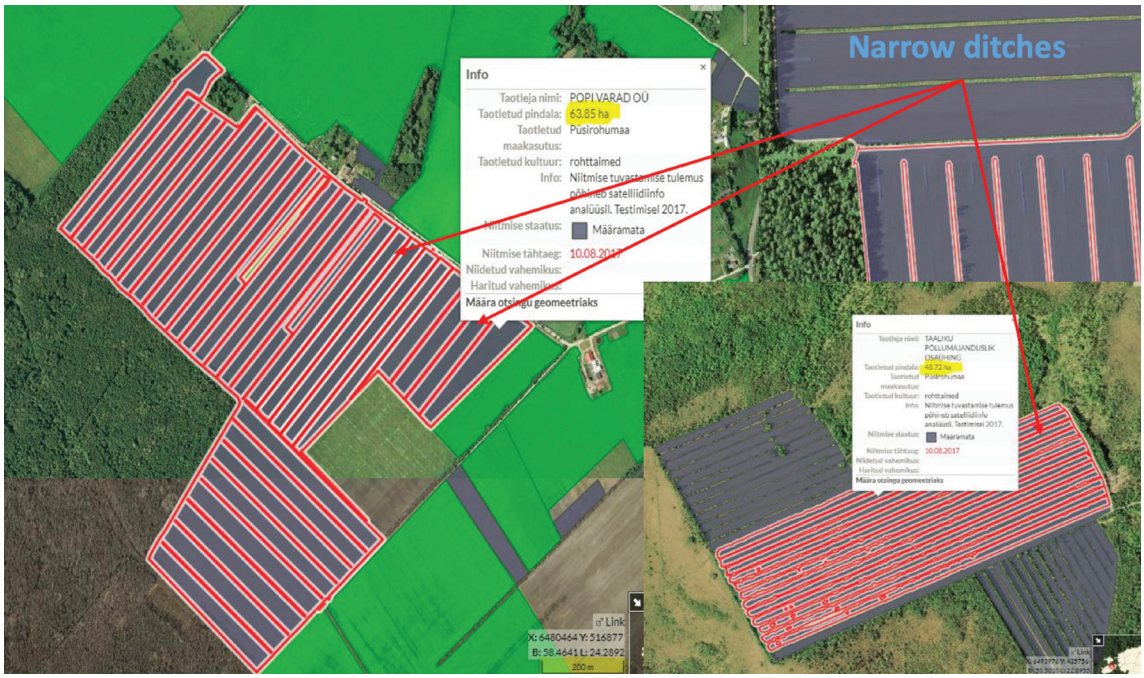
[43] ADB. 2021. *Harnessing the Potential of Big Data in Post-Pandemic Southeast Asia*. Manila.

Geospatial Data

Satellite imagery is one of the largest and most rapidly expanding sources of big data provided by governments. A study conducted by ADB has shown the potential of using satellite imagery to generate rich insights on poverty levels. In collaboration with Thailand and the Philippines' national statistics offices, it was found that using publicly accessible satellite imagery provided more granular predictions of poverty levels. The data enabled the governments to address COVID-19 issues and identify vulnerable households for food distribution.[44]

Another example of collaboration with the private sector on geospatial data imagery is Estonia's agriculture registers. Through an automated satellite-based information system (SATIKAS project), the Estonian government was able to use satellite data to determine whether grasslands have been mowed according to regulatory requirements. While the satellite imagery is owned by the government, the SATIKAS project partners with CGI, a private company, to develop the data infrastructure, software, and system integration (Figure 2).[45]

Figure 2: Satellite Imagery of Grasslands with Skipped Parcels for Mowing Detection



Source: A. Believe and K. Voormansik. 2018. *Satellite based grassland mowing detection*. Presentation for the Tallinn e-Governance Conference 2018. Tallinn. 29–30 May.

[44] Y. Sawada and E. Tan. 2020. Meeting development challenges with trusted data. *Asian Development Blog*. 20 October; A. Martinez and A. Mehta. 2020. How Satellite Data Helped Get Food to the Hungry during COVID-19. *Development Asia*. 21 December.

[45] OECD. 2021. *Chapter 13. Case Study 8: Estonia e-Government and the Creation of a Comprehensive Data Infrastructure for Public Services and Agriculture Policies Implementation*.

This project allows the government to analyze subsidized land and helps process new subsidy applications and data registrations. The adoption of this remote sensing and automation system enables monitoring activities to be conducted remotely, hence expanding the overall reach of the program. The project also includes a notification system to inform farmers who have not fulfilled their mowing and grazing requirements.[46]

As the system is connected to the e-Estonia program, government agencies can run credit checks to determine which farmers are eligible for subsidies. Overall, this geospatial collaboration between the public and private sectors offers cost-effectiveness in the long term.

Visualization Tools

As greater volumes of public data become available, comprehensive, and interoperable, the types of analysis that can be undertaken by government agencies and research institutions also becomes more sophisticated. Developing robust data visualization tools is crucial to helping governments translate the complex results of this analysis into easily readable information. This would aid in further securing stakeholder buy-in for data-related public expenditure, while improving government transparency and civil consensus-building for government policy making.

Governments can ensure that the data provided is comprehensible and tailored to the needs, concerns, and interests of its populations. Some governments have met the rising perception of public data as a public utility with redoubled efforts to tailor open government data reservoirs to the concerns of their populations. This also helps secure stakeholder buy-in, while further communicating that governments are alert to the needs of their citizens (Box 21).

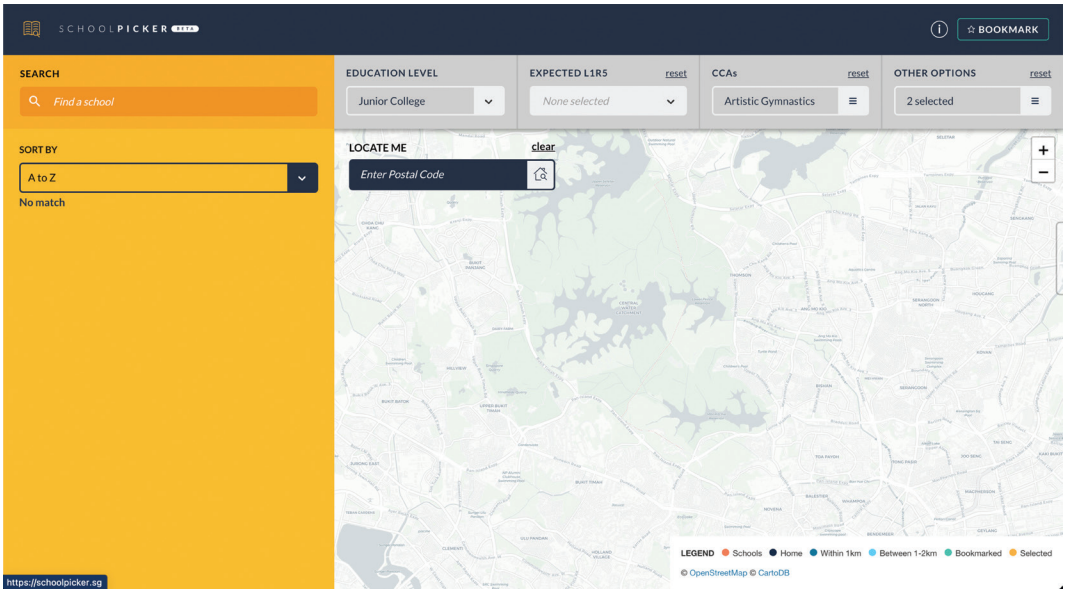
[46] Tartu Observatory. Information system SATIKAS helps to detect mowing by using satellite data.

Box 21: Tailoring Data-Driven Insights for Singaporean Parents

Established in 2002 as a joint initiative between the Estonian government, the United Nations Development Programme, and the Open Society Institute, the Estonian e-Governance Academy (eGA) functions as a nonprofit that aims to disseminate good digital government practices across the world through training, using Estonian and international best practices as a baseline for instruction. To date, the eGA has consulted with over 130 countries and trained over 3,000 officials across the world.[a]

Data.gov.sg powers several open government products which are tailored to the needs and concerns of ordinary Singaporeans. An example of this is the School Picker tool (Figure), which helps parents choose schools close to their homes, and which offer extracurricular programs which align with their children's interests.[b] This is an extremely useful tool given the widely acknowledged pressure many Singaporean parents experience in selecting schools for their children and reflects the Singapore government's interest in developing accessible data-powered solutions for citizens that can meet their needs and reflect the immense utility of data.

Figure: Singapore's School Picker Data Visualization Tool



Source: SchoolPicker. *Find a School*.

[a] Data.gov.sg. Government Technology Agency.
[b] Medium. Find the right school using our new School Picker tool.

Capacity Building

The speed at which governments can implement data management strategies and scale up the use of data hinges on whether public officers have acquired the necessary digital skills, and if they can comprehend the connection between data and digital technologies. Such skills range from basic digital hygiene, which can prevent avoidable security incidents, all the way to advanced development competencies which can aid governments in developing innovative data-derived service offerings and platforms to facilitate e-government service delivery. Briefings on digital fundamentals and the dissemination of best practices should be a priority as government systems become increasingly digitalized.

Appropriate steps should be taken to ensure that basic digital competencies are addressed, before scaling training procedures to address more advanced topics. Digital education initiatives can be introduced as part of civil service training curricula to fast-track adoption and comprehension of basic digital norms, especially those concerned with elementary data management principles such as security and storage procedures. Dedicated agencies can be established to focus on further skills training in conjunction with digital government-oriented organizations.

Incentives can be offered for government employees who develop viable digital skills, or who can create viable digital solutions. Facilities should be provided for public officers to acclimate to the use of digital platforms in workplace contexts, while internal contests, exercises, or hackathon events can be conducted to encourage further innovation.

Estonia's E-Governance Academy (eGA) is an excellent example of efforts to scale up digital and data competencies across government (Box 22).

Box 22: Building Whole-of-Government Competency with the Estonian e-Governance Academy

The Estonian e-Governance Academy (eGA) also created a handbook, *e-Governance in Practice*, a step-by-step guide to implementing digital government best practices. It is considered to be an authoritative text on developing viable digital government solutions and has been well received.[b] The academy also runs study visits, online courses, and continues to develop and release e-government publications in addition to its consulting services.[c]

As part of its mission statement, the eGA adapts Estonia's experience with digital government adoption to educate and train officials worldwide. This allows partner governments to benefit from lessons derived from its experience as a significant first-mover in digital government development. It also means that Estonia is exceptionally well positioned to shape narratives, best practices, and international standards regarding digital government implementation, an enviable position which affords it significant international prestige.

[a] H. Wright. 2020. Feature: How Estonia Is Helping Ukraine Develop e-Governance. *ERR News*. 4 September.
[b] S. Tambur. 2016. Estonian e-Governance Think Tank Launches a Guide to Digital Society. *Estonian World*. 14 June.
[c] e-Governance Academy.

Takeaways

To sum up, once there is a best practice framework in place with an aligned data strategy and stakeholder buy-in, the next step is to scale up data solutions. A multipronged approach is required to actualize this and should encompass the following aspects, which will mobilize partnerships between the public, private, and people sectors:

- Establish a dedicated digital agency
- A coherent and implementable data architecture
- Open government data
- Data marketplace
- Working with vendors
- Geospatial data
- Visualization tools
- Capacity building

Scaling up data requires vastly different organizational capabilities than implementing pilots and it is crucial that all government ministries and departments are ready to adapt to new ways of working. The approaches highlighted above will recenter organizational focus on people, technology, tools, and processes, with data at its core.

3 Conclusion

As digital technologies come to permeate every aspect of daily life, so too will more of our actions require and produce greater amounts of data. In several fundamental ways, it is becoming clear that countries or groupings of countries which are able to develop clear and effective data governance and management frameworks will shape the digital experiences of their populations. The principles with which they effectively leverage data inflows and outflows to their benefit will determine their success and ability for regional and global adoption of digital technologies. As this publication has shown, the effective deployment of data can result in tangible benefits for governments, including more effective service delivery and evidence-based policy making.

This publication identified and categorized approaches to effective data management and categorized them according to their function. Quick wins can create the momentum necessary for scaling up the use of data, but it must come with the implementation of rigorous governance mechanisms. In this way, the interests and engagement of stakeholders can be generated and lead to data-driven initiatives that can run on robust and secure data reservoirs.

This publication has highlighted specific national strategies and approaches to data management that can serve as useful signposts for governments in the process of developing their own approaches. It is hoped these case studies have provided both illustrative and aspirational examples of effective data management.

As a diverse region comprised of economies at different stages of digital development, the years to come will show whether the current digital divides will deepen or whether gaps can be addressed and challenges overcome. Countries that can better access and make good use of data may forge ahead swiftly, leaving behind others unable to do so. Cooperation and integration are desirable as all stand to benefit from data sharing, increased compatibility, and interoperability of digital systems and regulatory frameworks.

Nothing could have illustrated this more completely than the impact of the COVID-19 pandemic. As numbers began rising, countries that were able to rapidly deploy digital solutions and leverage data insights were the ones best able to control its spread. During the height of the pandemic, data contributed to the emergence of innovative digital solutions that continued to save lives, maintain economic activity, and facilitate interactions.

Enduring commitments must be made to ensure that data remains a resource to be readily catalyzed for societal benefit by both the public and private sectors. This will require innovative, proactive, and sustained action on the part of governments to ensure that the substantive data reservoirs they have at their disposal are managed responsibly and in accordance with international best practices. Clearly articulated and rigorously implemented data management principles and strategies are vital to ensuring this is the case.

APPENDIX

Country Case Studies

This section summarizes the progress made by three countries at various stages in their data management journeys.

Indonesia

Indonesia is the largest economy in the Association of Southeast Asian Nations (ASEAN). It has a massive population of over 250 million people and is home to over 10 tech unicorns.[1] Over multiple administrative terms, the Indonesian government has recognized the importance of fostering governance systems that effectively leverage digital technologies.

Emerging Market: Indonesia

- ✓ Strategic vision set by the President
- ✓ Open government data
- ✓ Activating improvements in government service delivery using open data

A Commitment to Transparency

Indonesia preceded its data management journey with declarations that strongly outlined a commitment to transparency. In 2008, Indonesia passed the Public Information Disclosure Act to improve transparency, and in 2011 became a founder of the Open Government Partnership, which aims to promote transparent, participatory, inclusive, and accountable governance.[2]

Within the following year, the government presented its first Open Government national action plan, which continues to be regularly updated with the most recent iteration addressing the period 2020–2022.[3] These national action plans provide overarching strategies which clearly articulate Indonesia's desire to improve its governance and refer specifically to the importance of open government data in bringing these improvements about.

This was an important first step by the government to rally internal stakeholders to align with a policy which advocated for greater government transparency, which would subsequently be translated to data management principles as digital transformation initiatives were rolled out.

---

1 L. Tan. 2022. Indonesia's start-up scene: The land of plenty. *FinanceAsia*. 1 November.

2 D. Setiawaty. 2017. Open Data Brings Change to Indonesia. *World Bank*. 31 January.

3 Open Government Indonesia. 2019. *Indonesia Open Government Partnership: National Action Plan 2020-2022*.

Implementing Open Government Data Initiatives

Ministries and national and local agencies in Indonesia do not have harmonized data reservoirs that are easily accessible due to challenges inherent to aligning different institutions which have until now maintained rigidly siloed approaches to data management. A coordinated effort involving local and central government agencies, institutions, and support from citizens was deemed necessary to break down these silos, and thus improve the overall quality of government service delivery.

Indonesia's first approach was to create a central data portal providing public access to more government data. The introduction of Satu Data Indonesia (One Data Indonesia) by President Joko Widodo in April 2016 was an important first step. Satu Data Indonesia was established to improve the quality of governance by improving the interoperability and accessibility of governmental data.[4]

Through facilitating wider access to government data, this initiative aims to integrate data-based approaches into government planning and budgeting efforts and inform comprehensive, evidence-based policy making across ministries and government agencies at both the national and local levels. Aligning with the Public Information Disclosure Act, the initiative was successfully passed after extensive examination as Presidential Regulation No. 39 of 2019 in June 2019. Satu Data Indonesia provides a common set of data standards for government agencies to follow, aiding significantly in intra-agency data sharing and common principles of data governance, with the powerful National Development Planning Agency being appointed to collect and harmonize data across agencies.

Building Coordinated Digital Government Approaches

The Indonesian government is aware of the importance of establishing data-driven digital service delivery platforms to enhance public access to government services. Indonesia's e-government implementation prior to 2018 was due a significant shift in philosophy.[5] Before 2018, government institutions implemented e-services that were conceived and developed internally, which eventually resulted in unpopular, unsustainable, or unintegrated service offerings.

The Ministry of Administrative Reform and Bureaucratic Reform study on Indonesia's e-government maturity level in 2018 revealed that the lack of an integrated and holistic e-government policy had led to fragmentary approaches to planning and implementing e-government.

Through analyzing approaches taken by more advanced countries in integrating e-services, such as the United Kingdom's gov.uk and the Republic of Korea's gov.kr, Indonesia worked to develop a similar national portal to include services provided by both central and local governments.

Initial steps have been taken to achieve this by leveraging the guiding principles set out in the E-Government Presidential Regulation No. 95/2018.[6] To develop its national portal, Indonesia

[4] Government of the Republic of Indonesia, Cabinet Secretariat. 2019. *President Jokowi Issues Regulation on One-Data Indonesia*. 27 June.

[5] A. A. Utama et al. 2020. The Implementation of e-Government in Indonesia. *Unair News*. 22 December.

[6] H. Rohman. 2020. Indonesia's Vision for Digital Government in 2025. *GovInsider*. 25 February.

has allocated Rp11 billion ($768,000) for its National Medium Term Development Plan 2020–2024.[7] The Ministry of Communications and Information has been tasked with managing the project.[8]

The United Nation's E-Government Development Index (EGDI) 2020 ranked Indonesia at 83 out of 193 countries, compared to its ranking of 107th in 2018 and 116th in 2016.[9] Inter-agency collaborations[10] and international partnerships, such as the Indonesia–Republic of Korea cooperation to accelerate the implementation of the Electronic-Based Government System, have had tangible impacts in helping to improve EGDI rankings.[11]

With steady progress made on a sturdy foundation of transparency and data sharing, Indonesia's approach to government digital transformation is off to a good start, and its ambitions for a national portal may soon become a reality as services continue to be rolled out in a more integrated and cohesive fashion.

Japan

Progressive Market: Japan

- ✓ Mature personal data protection and cybersecurity regulation
- ✓ New national strategy and stand-alone digital agency
- ✓ Quick wins

Japan is known for adopting progressive and forward-thinking policies on data management. It was the first country to be granted data protection adequacy determination by the European Commission, meaning that the country has been judged to maintain sufficiently stringent provisions that European Union data can be allowed to enter Japan under the General Data Protection Regulation (GDPR) with minimal additional oversight.[12] However, Japan lags in terms of a cohesive data management architecture and a relative lack of initiatives aimed at scaling up the use of data.

Trailblazing and Building on Approaches to Personal Data Protection

An early mover in the regulatory space, Japan began the process of creating legislation for both personal data protection and cybersecurity in 1999. The government would ultimately publish its Act on the Protection of Personal Information (Law No. 57, May 30, 2003) (APPI) in 2003.[13]

---

7 Rp1 = $0.000064; Government of the Republic of Indonesia, Cabinet Secretariat. 2020. Gov't Issues Regulation on 2020-2024 National Medium-Term Development Plan. 13 February.

8 J. Kelleher. 2017. Implementation of e-Government to Be Accelerated in Indonesia. *OpenGov Asia*. 17 October.

9 UN E-Government Knowledgebase. Indonesia (accessed 3 December 2021).

10 F. Ludiana. 2020. Year-end notes 2020: Realizing the President's Vision and Mission, Ministry of PANRB Achieves A Number of Achievements. *The Ministry of Administrative and Bureaucratic Reform*. 29 December.

11 Government of Indonesia, Ministry of Administrative Reform and Bureaucratic Reform. 2021. In Collaboration with Korea, the government focus on developing E-Government.

12 European Commission. 2019. *European Commission adopts adequacy decision on Japan, creating the world's largest area of safe data flows*. 23 January.

13 Personal Information Protection Act (Act No. 57 of 2003).

Reflecting the government's commitment to ongoing improvements to its regulatory regimes, the APPI was subsequently updated in 2016 to account for changes in technological advancements and the internet.[14] Amendments to the APPI defined personal information in a more detailed manner and introduced newly defined data categories such as "sensitive personal information" and "de-identified information".

Under the amended APPI, Japan also improved measures to safely facilitate cross-border data flows and established the Personal Information Protection Commission to centralize the management of data protection. More recently, new amendments have introduced vigorous measures aimed at tackling data breaches and improving processes to allow cross-border transfer of information, which will come into effect in 2022.[15]

Establishing Strong Cybersecurity Foundations

Recognizing early on the importance of cybersecurity to the development of the growing digital economy, Japan rapidly established several cybersecurity strategies, culminating in the passage of the influential basic act on Cybersecurity in 2014, which codified government-wide approaches to cybersecurity management and aimed to enhance cybersecurity standards and organizational cooperation.[16] The Basic Act has since been revised twice to reflect changing cyber-threat profiles, including the escalation of data breaches and the proliferation of ransomware attacks.

The IT Security Office, which eventually became the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), laid the groundwork for both public and private sector stakeholders by issuing detailed guidance on best practices and preferred approaches.[17] Until the Basic Act on Cybersecurity was passed, major national policy making on cybersecurity was undertaken through the issuance of national strategies on information security, overseen by the Information Security Policy Council and the NISC.[18]

Using these national strategies, the government implemented measures and action plans to protect critical infrastructure and government computer systems. The Cyber Security Strategic Headquarters was established in 2014 with the Basic Act on Cybersecurity and was placed under the direct oversight of the Prime Minister.

[14] Personal Information Protection Commission, Amended Act of Personal Information, 2016.

[15] Personal Information Protection Commission, Amended Act of Personal Information, Japan. 2020.

[16] Japanese Law Translation. 2020. The Basic Act on Cybersecurity. 13 October.

[17] National Center of Incident Readiness and Strategy for Cybersecurity, History of Governmental Framework on Cybersecurity, Japan (accessed 3 December 2021).

[18] B. Benjamin. 2019. *How Japanese Cybersecurity Policy Changes*. Weatherhead Center for International Affairs Harvard University. Massachusetts.

Securing Public Buy-In through Contests

To secure stakeholder buy-in, the Japanese government has been actively launching public contests to promote its data management messaging as a quick win. The Tokyo Metropolitan Government and several ministries co-host and support the Association for Open Data of Public Transportation's Open Data Challenge for Public Transportation in Tokyo.[19] The competition aims to promote the development of projects to use public transportation data to develop applications that enhance user convenience.

The latest contest, held in 2018, was the fourth iteration and supported the Japanese government's agenda of providing applications for visitors in Tokyo during the 2020 Olympics. Some applications allowed users to easily access information on train timetables and transfers in Tokyo, locate public toilets close to bus stops, and find transfer routes for Olympic venues.

Using such approaches, the Japanese government has catalyzed interest and investments in open data, while bringing greater public attention to its broader data management philosophy.

Strategic Responses to Crisis Management

Despite having basic legislation related to data management and a proactive approach to courting stakeholder engagement, Japan's civil service has been slow to fully adopt digital transformation measures. One element of resistance is the cultural preference for traditional stamps (Hanko) for official documents, using fax machines to send reports, and a reluctance to adopt digital payments stemming from several high-profile payment system failures. Nevertheless, there have been a series of crises that have accelerated calls for rapid digitalization.

Japan's information and communication technology (ICT) systems for disaster response and recovery were tested during the Great East Japan Earthquake in 2012.[20] The incident highlighted the need for progressive measures on opening access to government data to increase public and private sector coordination and improve private sector services. This led to the IT Strategic Headquarters adopting the Open Government Data Strategy, which, in 2013, led to the launch of the open government portal data.go.jp.[21]

More recently, the coronavirus disease (COVID-19) pandemic demonstrated how Japan's slow uptake of digital services has impeded its ability to quickly react to a crisis.[22] The pandemic catalyzed the government's resolve to accelerate digital transformation, which led to the creation of a National Data Strategy which outlines action plans for data coordination, distribution, and database registry.[23] Under the strategy, Japan plans to conduct studies on a data marketplace to establish specific regulations and standards to establish such a platform in the future.

[19] Tokyo Public Transportation Open Data Challenge. Open Data Challenge for Public Transportation in Tokyo.

[20] K. Sakoda et al. 2021. Learning from Megadisasters: A Decade of Lessons from the Great East Japan Earthquake. World Bank. 11 March.

[21] Government of Japan, Prime Minister Office of Japan. 2012. *Open Government Data Strategy*. Tokyo.

[22] J. Ryall. 2020. Japanese decry boomer-era tech as hospitals file coronavirus cases by fax. 5 May.

[23] Government of Japan, National Strategy Office of IT, Cabinet's Secretariat. 2021. National Data Strategy. Tokyo.

A Digital Agency for a Digital Government

In arguably the strongest reflection of the cultural shift taking place across the Japanese government, a stand-alone digital agency was announced in late 2020, with the agency officially coming online a year later in September 2021.[24] Without a central control office, public agencies struggled with creating harmonized data management systems and coordinating data-sharing efforts for digital government services. Established under the Cabinet and overseen by the Prime Minister and a specially appointed minister for digital affairs, the digital agency has been granted the authority to supervise all the basic policies and measures for data governance and overall digital transformation across the Japanese government.

Although at too early a stage to comprehensively assess, the digital agency is promoting various policies to expand digital reform, such as expanding digital certificates and signature systems, and adopting cloud services for public agencies.[25] The digital agency announced a government cloud computing project supported by global service providers to accelerate the digitalization of nationwide government information systems.[26]

Starting with a select few municipalities during a trial period, the project is expected to consolidate government data management systems more efficiently in both function and cost, serving as a critical mechanism for facilitating a faster digital transition and providing for more inclusive and holistic e-government services.

Republic of Korea

The Republic of Korea is home to one of the world's most advanced digital governments. The Organisation for Economic Co-operation and Development (OECD) Survey on Digital Government ranks the Republic of Korea first in the world to be a government reliant on 'digital by design' principles, meaning that the government integrates digital technologies as the founding mechanisms for public information systems.[27]

Progressive Market: Republic of Korea

- ✓ National strategy
- ✓ Open government data
- ✓ Personal data protection and cybersecurity regulations
- ✓ Upcoming National Data Policy Committee

The Republic of Korea also maintains high rankings in the United Nations (UN) e-Government Survey and was ranked as the top country in e-government development in 2010, 2012, and 2014, most recently being ranked second in the world in 2020.[28] These laudable achievements have been made

[24] Internet version of Kanpo (accessed 3 December 2021).

[25] Government of Japan, The Digital Agency. Policy.

[26] Press Conference by Minister Makishima on 26 October, 3rd year of Reiwa (accessed 3 December 2021).

[27] OECD. 2020. *Digital Government Index*.

[28] UN Department of Economic and Social Affairs. 2020. *E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development*. New York.

possible by initiatives for the digital transformation of government administration services that have been developed and proactively implemented since the 1990s.

From Data Management Infrastructure to Open Government

The Republic of Korea's Ministry of Information and Communication, today the Ministry of Science and ICT (MSIT), was established in 1994, with the passage of the Framework Act on Promotion of Informatization.[29] The focus of the framework act was the digitization of major national administrative services and the creation of a basis for information sharing, along with the development of intra-government digital infrastructure.[30] The government further enacted the Regulations on Sharing Administrative Information and the Digital Signature Act to support these policies.[31]

In the early 2000s, the Korean government began more actively promoting its national e-government development plans. The e-Government Act was passed in 2001 and established a special committee on e-government under the President to elevate the e-government initiative as a Presidential Agenda (footnote 31). The government also began publishing its Master Plan on National Informatization every 5 years and launched various initiatives, including the Republic of Korea's first integrated government data center in 2005.

By the 2010s, the government's focus shifted from enforcing the digitalization of government-to-government services to promoting the digitalization of government-to-citizen services. Relevant initiatives included the launch of the integrated government service portal, Gov24, and the online tax service portal, HomeTax, in the late 2010 (footnote 31). In 2013, the government established a basis for releasing government data to the public by enacting the Act on Promotion of the Provision and Use of Public Data. This helped to establish the open government data portal, data.go.kr, which allowed public users and businesses to easily access data from various government agencies through a centralized portal.[32]

Widening Regulatory Tool Kits

Alongside these proactive ventures into digital government, the Republic of Korea also made considerable progress in establishing personal data protection laws and developing its cybersecurity regime. The issue of personal data protection emerged as a critical agenda item when the government was enforcing its e-government initiatives in the early 2000s.

Discussions on introducing a legislative framework to address personal information started in 2003. The first Personal Information Protection Act (PIPA) was formally passed in 2011, and a Personal Information Protection Committee was created to govern personal data protection regulations (footnote 32). Since then, a major amendment to the PIPA in 2020 introduced new categories of

[29] C. Chung. Informatization and e-Government Policy in Korea. 30 years of change.

[30] Government of the Republic of Korea, Ministry of Public Administration and Security. 2017. *50 Years of E-Government in Korea (1967–2017)*. Seoul.

[31] Government of the Republic of Korea, Ministry of the Interior and Safety. 2020. *Digital Government: Republic of Korea*. Seoul.

[32] Government of the Republic of Korea, Ministry of Government Administration and Home Affairs. 2016. *e-Government 2020 Master Plan*. Seoul.

data, such as pseudonymized and anonymized data, and provided the legal basis for processing pseudonymized data to promote its use. Such progress paved the way for the Republic of Korea to become the second Asian country after Japan to be issued an adequacy determination under the European Commission's GDPR.[33]

MSIT is currently preparing a Framework Act on Cybersecurity based on its national cybersecurity master plan to secure national infrastructure, personal data, and network systems.[34]

Promoting the Data Industry

While the administration established a national plan for data industry promotion, the momentum to mature a data-specific national strategy was gradually lost as interest shifted to consolidating diverse and overlapping digital policies.[35] Despite this, the Framework Act on the Promotion of Data Utilization and Industry (Data Framework Act) was deliberated and is expected to be enacted in 2022. Under the Data Framework Act, a National Data Policy Committee will be established to manage overall national policies for both public and private data. The committee will also publish a master plan on data industry promotion every 3 years, providing new opportunities to develop advanced data management practices.

Cloud-Oriented Digital Transformation Measures

Acknowledging the importance of cloud transformation to accelerate advancements in public data governance and e-government services, various administrations adopted initiatives to establish cloud infrastructure for public agencies. In 2013, the government created the Government 3.0 Cloud Process Plan, which aimed to establish cloud storage and cloud-based public computing and information centers (footnote 30).

The government also developed security measures to ensure the secure use of cloud services in the public sector. The Cloud Security Assurance Program is a certification requirement released in 2018 for the public sector to use commercial cloud services, and this has facilitated the government's transition to cloud computing in its early days of adoption. In 2020, the government included cloud computing as one of the sub-areas for its Digital New Deal[36] projects to transition to cloud services through state-led projects and investments and aims to achieve 100% cloud transformation of administrative and public agencies by 2025.[37]

This general support for cloud services is also receiving substantial support from the MSIT, which issued its third Cloud Computing Master Plan in September 2021.[38] Unlike the previous initiatives, the current

[33] European Commission. 2021. Data Protection: European Commission Launches the Process towards Adoption of the Adequacy Decision for the Republic of Korea. Press release. 16 June.

[34] Government of the Republic of Korea, Ministry of Science and ICT. 2020. Preliminary Information Disclosure List. 8 April.

[35] J. Jun-Hwa. 2018. The Current State and Challenges of Data Policy Governance.

[36] Government of the Republic of Korea. 2020. *Korean New Deal: National Strategy for a Great Transformation*. Seoul.

[37] Government of the Republic of Korea, Ministry of the Interior and Safety. 2021. *Transition to Internet-based resource sharing (cloud) of all administrative and public institution information systems by 2025*. 26 July.

[38] Government of the Republic of Korea, Ministry of Science and ICT. *14th Information and Communication Strategy Committee*.

plan focuses on expediting the urgent adoption of public cloud services given the weaknesses in existing digital infrastructure revealed during the COVID-19 pandemic.

The Republic of Korea's leading role among digital governments reflects the cohesive and sophisticated strategies put in place across the past few decades to ensure that internal government data management infrastructure was adequately advanced before digital government initiatives were formally pursued. Its progress thus stands as a testament to the need for adaptability and strong fundamentals in data management, and to digital government implementation.

Data Management Policies and Practices in Government

This report shows the benefits of effective data deployment, highlights national data management strategies, and shows how governments in the Asia and Pacific region can use data driven approaches to improve governance and growth. Sketching out a roadmap and using case studies, it shows how governments can conceptualize, create, and implement data management policies and practices. It emphasizes the need to get stakeholder buy-in, scale-up data use and ensure it is regulated and secure. It highlights why strong data management is critical for boosting governance and shows the need to better access and use data to bridge the digital divide.

About the Asian Development Bank

ADB is committed to achieving a prosperous, inclusive, resilient, and sustainable Asia and the Pacific, while sustaining its efforts to eradicate extreme poverty. Established in 1966, it is owned by 68 members —49 from the region. Its main instruments for helping its developing member countries are policy dialogue, loans, equity investments, guarantees, grants, and technical assistance.

About the AWS Institute

The Amazon Web Services (AWS) Institute is a thought leadership and executive education program to accelerate digital transformation for public sector executives.

AWS INSTITUTE

ASIAN DEVELOPMENT BANK
6 ADB Avenue, Mandaluyong City
1550 Metro Manila, Philippines
www.adb.org