Building & Securing Digital Public Infrastructure

A playbook for local and regional governments

UN HABITAT
FOR A BETTER URBAN FUTURE

UN HABITAT
FOR A BETTER URBAN FUTURE

Building and Securing Digital Public Infrastructure
A playbook for local and regional governments

United Nations Human Settlements Programme (UN-Habitat)
P.O. Box 30030 00100 Nairobi GPO KENYA
Tel: 254-020-7623120 (Central Office)
www.unhabitat.org

HS/044/21E

Cover photo © PR Image Factory / Shutterstock.com

Acknowledgements
Project supervisors: Katja Schaefer, Pontus Westerberg
Principal author: Emily Royall
Contributors: Livia Schaeffer Nonose, Miles Nathan Lewis Andres Vecchio
Peer reviewers: Frédéric Saliez, Fernando Almeida, Melissa Permezel
Design and layout: Austin Ogola

Contents

Chapters

Tables

Boxes

Foreword

Ms. Maimunah Mohd Sharif

Under-Secretary-General and Executive Director, United Nations Human Settlements Programme (UN-Habitat)

As the agency with the mandate to coordinate urbanisation matters within the UN System, UN-Habitat often highlights that half the world's population - 3.5 billion people - now live in cities. The world is both urbanising and digitising at a rapid pace and we see that digital technologies have great potential to assist Member States in their efforts to achieve sustainable urban development. The 'smart city' as a concept is the lynchpin connecting these two global mega-trends. It can help Member States achieve positive transformative change by harnessing ICTs and digital technologies to improve urban efficiency, quality of life and sustainability.

Whilst digital technology can have enormous transformative potential for positive change, it can also perpetuate existing social and economic inequalities. In 2020, I saw many children struggle to get 'connected' including the students in my rural village with many missing out on their educational needs.

To address this yawning digital divide, the UN Secretary-General has made a strong case for human rights in digital spaces in his 2020 Roadmap for Digital Cooperation, which lays out key areas for action including universal connectivity, promoting digital public goods, and ensuring trust and security in the digital environment. Additionally, in the Connect 2030 Agenda, our colleagues at ITU commit to bridging the digital divide for an inclusive information society and enabling the provision of broadband access for all, leaving no one offline.

For UN-Habitat, the use of digital technologies in cities and by cities must be appropriate to ensure that the prosperity they bring is shared among urban residents, cities and regions. Ultimately, the deployment of technology needs to be grounded in the real needs of people. It should pay particular attention to underserved populations in order to address inequalities and bridge social and spatial divides. Our people-centered smart cities flagship programme was launched in 2020 to provide strategic and technical advice to local, regional and national governments to enable them to take a strategic and proactive approach to digital transformation, while meaningfully engaging their residents and ensuring human rights in digital spaces.

We must address the elephant in the room. People-centered smart cities cannot be built when so many remain outside of the digital world. The people-centered smart cities Playbook Series aims to help cities and communities ensure that urban digital transformation works for the benefit of all, driving sustainability, inclusion and prosperity in the process. Each playbook in the series represents one of five Pillars of People-Centered Smart City development: Community, Digital Equity, Infrastructure, Security and Capacity. Collectively, the playbooks outline key activities, provide recommended actions, and policy toolkits that provide actionable guidance for cities seeking to ensure a more equitable, inclusive and sustainable future for smart cities.

About UN-Habitat

The United Nations Human Settlements Programme (UN-Habitat) is the United Nations programme working towards a better urban future. Our mission is to promote socially and environmentally sustainable human settlements development and the achievement of adequate shelter for all. We work with partners to build inclusive, safe, resilient and sustainable cities and communities and promote urbanization as a positive transformative force for people and communities, reducing inequality, discrimination and poverty. UN-Habitat provides technical assistance, policy advice, knowledge and capacity building to national and local governments in over 90 countries.

UN-Habitat is coordinating the implementation of the UN System-Wide Strategy on Sustainable Urban Development[1] and in close coordination with national and local governments, the agency leads the monitoring of Sustainable Development Goal 11 (SDG11) on sustainable cities and communities as well as the New Urban Agenda.

UN-Habitat's approach to people-centered smart cities

Launched in 2020, UN-Habitat's flagship programme 'people-centered smart cities' acknowledges the transformative potential that digital technologies can have for sustainable urban development. Through the people-centered smart cities flagship programme, UN-Habitat provides strategic and technical support on **digital transformation** to national, regional and local governments.

Digital transformation is now critical to meet the demands of sustainable urban development. In the past decade, internet connectivity has become a requisite for full participation in society, including access to education, affordable housing, and critical government services -- yet 3.7 billion people were offline in 2019[2]. In recent years, digital innovations like civic technology, geographic information systems, the sharing economy, open data, and digital platforms have changed how people understand, manage and participate in cities. The COVID-19 pandemic introduced even greater urgency for local and national governments alike to bridge the digital divide especially for marginalized groups and informal settlement communities[3], build more efficient and secure data management systems, and protect citizens' privacy when using digital services. These activities are the foundation for inclusive and resilient smart cities.

Unfortunately, many 'smart city' initiatives have fallen short on sustainability, where technology has been applied uncritically, based on supply rather than demand. Investments in smart city projects that prioritize technology's capabilities over residents' needs have not delivered expected impacts. Instead, we see trends towards surveillance, private ownership of digital public goods and infrastructure, and the perpetuation of discrimination through automated decision-making powered by artificial intelligence. As cities have become testing sites for these new technologies, there is growing concern about a lack of oversight, transparency, and potential human rights violations in smart city frameworks.

Smart cities can have a tremendous positive impact on people's lives, but only when people are at the center of the development process. This is why UN-Habitat is introducing the '**people-centered smart cities**' approach, which aims to show how smart cities can be an inclusive force for good, if implemented with a firm commitment to improving people's lives and building city systems that truly serve their communities. This requires engaging deeply with the needs of all residents and urban stakeholders through meaningful community participation, bridging the digital divide, developing essential digital infrastructure and governance, and building capacity through multi-stakeholder partnerships. It also requires governments to take a strategic approach to digital transformation, understanding its potential, and ensuring that it aligns with existing priorities as outlined in the 2030 Agenda for Sustainable Development, including sustainable transport, inclusive neighbourhood planning, providing affordable housing and reducing carbon emissions.

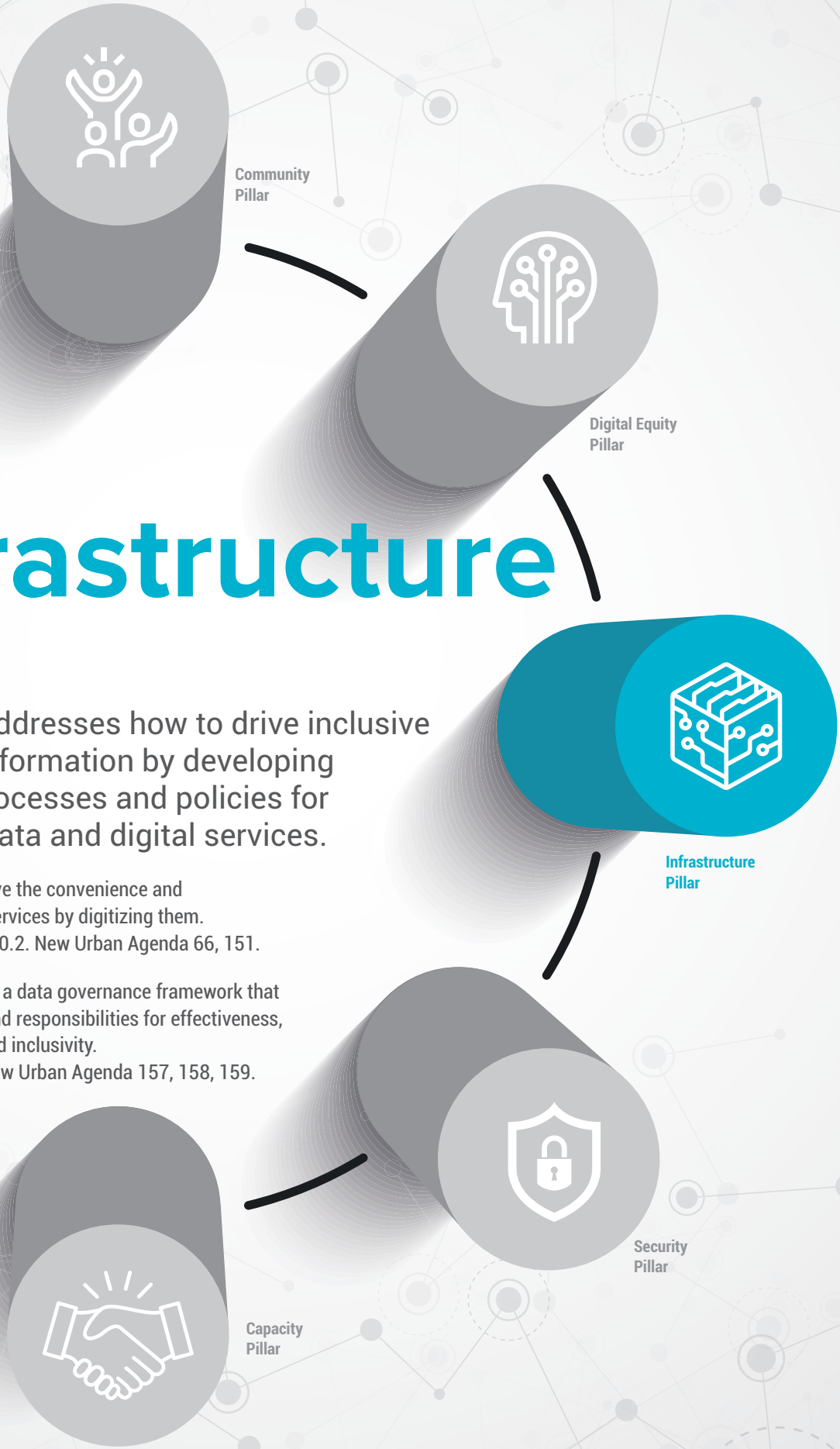
This new series of playbooks is a key normative component of UN-Habitat's people-centered smart cities flagship programme that aims to empower local governments to take a **multi-stakeholder approach to digital transformation that realizes sustainability, inclusivity, prosperity and human rights for the benefit of all.** To that end, local, regional and national governments will find pragmatic guidance for how to develop smart city strategies that are more inclusive, sustainable, and aligned to the actual needs of residents. We look forward to working with a wide variety of partners to implement the recommendations from the playbooks in a collaborative manner.

3.7 billion people

were offline in 2019

In the past decade, internet connectivity has become a requisite for full participation in society, including access to education, affordable housing, and critical government services.

Pillars of a people-centered smart city



Infrastructure Pillar

This pillar addresses how to drive inclusive digital transformation by developing systems, processes and policies for managing data and digital services.

- **Activity 5:** Improve the convenience and accessibility of services by digitizing them. SDG 5, 5.B., 10, 10.2. New Urban Agenda 66, 151.
- **Activity 6:** Create a data governance framework that sets standards and responsibilities for effectiveness, accountability and inclusivity. SDG 16, 16.6. New Urban Agenda 157, 158, 159.

Security Pillar

This pillar addresses how local governments and national governments can work in unison to achieve secure smart city assets including data and infrastructure in order to improve public trust.

- **Activity 7:** Safeguard public trust by protecting smart city assets.
- SDG 16, 16.6. New Urban Agenda 157.

Who is this playbook for?

This playbook is for local, **regional, and national governments, policymakers, civil society, and non-governmental organisations** operating in urban and rural environments seeking practical methods to develop systems, processes and policies for digital transformation while prioritising security and public trust. This playbook provides these groups with support to contextualise their efforts within the broader framework of the UN's resolutions, the Sustainable Development Goals, the New Urban Agenda, and follows the core values outlined under the Digital Infrastructure and Security Pillars in *Centering People in Smart Cities: A Playbook for Local and Regional Governments*. It also includes case studies from around the world and sample policy toolkits for key areas. At the end of this playbook, readers should have a basic understanding of how to operationalize people-centred smart cities through inclusive digital transformation that secures smart city assets, and builds public trust.

01

Introduction to the playbook

Traditionally, infrastructure has referred to physical systems like roads, sidewalks, and power grids that underpin daily life in cities. Throughout modern history, urban planners have developed codes, standards, and policies to make these systems more efficient and to protect them, and the citizens that use them, from harm. Today, local and national governments are facing a new layer of public infrastructure that is taking precedence over how cities control, manage, and understand the systems they operate: **digital infrastructure**. In the context of this playbook, digital infrastructure refers to the tools and systems required to make digital life function in cities. Digital infrastructure as a public service, or digital public infrastructure, lets us experience and monitor city services, and engage in civic life through the use of the internet and online transactions.

The process of using technology to build digital infrastructure to improve operational performance is called **digital transformation**. Digital transformation is new and as a result, it presents tremendous opportunities and risks to local and national governments, as well as the people they serve. For example, as governments introduce new and sometimes unproven technologies for building services, they can also introduce new risks to residents' privacy and security. Recent case studies have shown that the use of technology in smart cities can also erode social protections, deepen inequalities and exacerbate existing discrimination, such as through the use of facial recognition or artificial intelligence in automated decision-making[4]. This is especially true for marginalised groups including women, LGBTQIA + communities, refugees and persons on the move, the elderly, and those who have been left behind. **Consequently, building digital infrastructure must be treated as a socio-cultural challenge, just as much as a technical one.**

The process of digital transformation varies with the unique cultural and economic context of every city. Therefore, city governments that want to develop or improve digital services should first work with residents to establish standards for how digital services should address their lived experiences. These **digital service standards** become a set of best-practice principles for designing and delivering government services. Section 02 covers what should be included in a digital service standard, and how to create the necessary buy-in from both city leadership and the community to ensure their utility and success.

Once community guidelines are set for developing and delivering digital services, the infrastructure that supports them must be built. Section 02 covers three major types of protocols that facilitate digital public infrastructure: digital identity, digital payments and data exchange. Collectively, we refer to these as the **civic technology stack**. City and national governments around the world have experimented with these protocols with varying degrees of success. This section evaluates these protocols from a people-centred smart city lens through privacy, equity, transparency and user-centred design. A variety of services can be powered by a civic technology stack, including taxation, benefits allocation, land titling, and procurement, among others.

The civic technology stack is not possible without data. How data is collected, managed and secured is critical to the success of digital public infrastructure, including payments and digital identity. Section 03 addresses **data governance** and provides guidance for how to build a data governance policy that sets standards and responsibilities for effectiveness, accountability and inclusivity. Data governance is more than a policy document, it's also a practice of sharing[5]. Likewise, this section provides information for how to translate data governance policy into action through programming, community engagement and training.

The final step in developing robust digital public infrastructure is ensuring that digital public infrastructure, and the data that supports it, is secure. Cybersecurity threats to local and national governments have become increasingly prevalent in recent years, further emphasising the need for cities to act. However, cybersecurity laws and policies have a direct impact on human rights, such as the right to privacy, freedom of expression, and the free flow of information[6]. While cybersecurity laws focus on introducing policies to protect sensitive information, they can also introduce provisions that threaten citizens' privacy or increase censorship[78]. City governments should take care to educate residents on cybersecurity issues, be transparent about adopted cybersecurity policies or laws, and take a human-rights approach to cybersecurity strategy.

This Playbook is broken down into three **activities** that support the Infrastructure and Security pillars of the people-centred smart city approach by UN-Habitat. Each activity includes **core values** that should inform your process and overall organisational culture, and strategic **goals** that your organisation can adopt to drive forward your people-centred smart city approach. For each goal, we outline a series of actions, recommendations and case studies that will help you take action right away. Finally, we end each activity with a policy toolkit, that highlights model policies you can draw inspiration from or adapt for your own context.

02

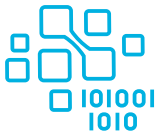
ACTIVITY 5:

Improve the convenience & accessibility of services by digitising them

SDG 5, 5.B., 10, 10.2.
New Urban Agenda 66, 151

Core Values

1 Digitization



Value 1: Digitization of public services can build public trust by increasing the accessibility, convenience and efficiency of basic services.

2 Open source platforms

Value 2: Modular, interoperable, and open source platforms can address core public sector challenges in key areas like digital payments, digital identity, and digital data exchange.

3 Digital equity

Value 3: When digitising a service, local governments should pay special attention to the many ways different types of people find, access, and use a service, by prioritising user-centred design and digital equity.

4 Privacy and security

Value 4: Privacy and security must be prioritised when developing digital government platforms.

Introduction

For local and national governments, **Digital transformation** refers to how organisations leverage technology to build public services that are convenient, more efficient, accessible, and secure for everyone. In order to effectively harness technology to improve public services, local governments need to target their limited resources to the most impactful areas of digital transformation, centre the design of those services on the end user, and prioritise privacy, transparency and security throughout the process.

Digitization presents exciting opportunities for cities, but can also introduce privacy, ethics and security challenges. The digital transformation process can also create more confusion if there is a lack of buy-in from leadership or employees, or coordination issues regarding contracts, staff and data accessibility. **When digitising public services, governments should ensure that these efforts are aligned with the SDGs, and respond to the actual needs and lived experiences of residents.** This can be accomplished by taking a multi-stakeholder governance approach to leveraging open source tools, interoperable platforms, and user-centred design for service development and delivery.

Digital government is increasingly popular, and makes particular sense in our post-pandemic reality that has increased demand for remotely accessible services. Some governments use their digital transformation as an opportunity to stimulate collaboration with communities of practice, such as the Taiwan Digital Ministry's Public Digital Innovation Space and the City of Recife's Open Innovation and Government Programme. Estonia's X-Road system offers transparent, open-source approaches to handling digital identity and technology development. Other efforts such as the World Food Program's (WFP) Building Blocks prioritises the needs of specific marginalised groups including underbanked refugees. Some governments focus on safely sharing data across stakeholders to improve service delivery, for example Germany's construction of shared digital infrastructure to standardised electronic medical records. How you prioritise your organisation's digital transformation depends on the needs of your community and resources at your disposal.

Digital government is increasingly popular, and makes particular sense in our post-pandemic reality that has increased

demand for remotely accessible services.

Transforming government culture and reforming legacy systems while keeping up with the pace of innovation in the technology sector can be extremely challenging for governments. This section of the playbook identifies several goals that local governments should undertake when initiating digital transformation in their organisation. These goals fall under three key areas that are foundational to any digital transformation effort:

1. **Establish digital service standards -** Digital service standards provide uniform commitments across all digital services provided by your organisation covering privacy, equity, security, and interoperability, among other things. Digital service standards create a guideline for any department seeking to improve or deliver a digital public service.

2. **Build your civic technology stack -** The civic technology stack refers to key areas of digital transformation for local governments namely digital identity, digital payments and data exchange. Each of these areas forms a layer of digital transformation that comprises the "stack."

3. **Build capacity and governance for your government's digital transformation -** Any digital service that is built must be maintained and supported by a management structure that ensures the longevity of the service. How you 'govern' digital transformation will look different for different communities, but all models should centre on transparency and collaboration.

GOAL #1 Establish Digital Service Standards to guide your approach to digital services across the organisation

Increasingly, **digital services** or how organisations provide services online, have become the front door for governments. However, every community has different values for the roles that government and technology play in their lives. For example, some communities with a diverse population may prioritise providing services in several languages, while others place more emphasis on ensuring privacy is protected for online transactions.

Local governments looking to build or improve digital services, should start by building **digital service standards** that reflect their community's priorities. Digital service standards are a set of best-practice principles for designing and delivering digital government services. Digital service standards typically apply to public facing services provided by a local government, and can be useful for any developer responsible for building a public facing digital service. Digital service standards can be developed by all levels of government. For example, Australia's Digital Service Standard applies to all national government services, Ontario's standards as part of the *Simpler, Faster, Better Services Act* apply to all public sector organisations, and Barcelona's Ethical Digital Standards covers those services issued by the local government. Digital service standards are critical for people-centred smart cities, because they focus on how services can be designed and delivered in ways that prioritise people's real needs and respect their lived experiences.

BOX 1.1

Ontario's Simpler, Faster, Better Services Act

HarassMap is a volunteer-run initiative which began in Egypt in 2010 with the goal of mapping out where sexual harassment occurs - with anyone allowed to anonymously mark the locations of, and describe, relevant incidents. HarassMap is largely a Cairo initiative to this day, with the vast majority of data points found in and around the city. The map of data points produced collectively by its users produces a sort of "heat map" of sexual harassment in Egypt, showcasing the extent of the problem and hot-spots of activity. It also allows users to mark and describe interventions to sexual harassment, showing users that both sexual harassment and intervening in sexual harrassment are quite common. With limited official response to this problem and with victims' discussion relatively taboo, crowdsourcing with victims able to post anonymously, allows data collection at a greater scale. HarassMap has also produced valuable research on sexual harassment in Egypt. HarassMap has worked with educational institutions and non-governmental organizations (NGOs), and organized workshops and campaigns against sexual harassment across Egypt. HarassMap has served as a blueprint for projects worldwide, and showcases a situation in which a crowdsourcing platform can set the stage for real social change.

What should be in digital service standards?

While digital service standards vary by community, there are consistent trends across standards currently offered by national, regional, and local governments alike. Broadly, digital service standards provide guidelines for how technology is developed in such a way that makes it easy to use, responsive, and accessible. Standards also help provide important requirements for security and protocols for managing data that is used, collected or generated by the service. Finally, digital service standards help minimise redundancy of a service, ensuring that it is **interoperable** or can "talk to" other existing services and systems managed by the organisation.

What follows are key elements that should be part of any digital service standard. Some of these are adapted from the global Digital Standard, developed by an independent coalition of open-source developers that provides developers with clear guidance for establishing digital service standards. The coalition welcomes contributions as digital services evolve, and are reviewed quarterly.

Privacy

Participating in digital transactions and services can introduce privacy risks for residents, especially as the nature of many government services can be very personal. Depending on how the service is built, sensitive data can be passed along to third party groups for processing. At every step of the way, sensitive or personal data must be secured, and users should at least be informed of how the data is processed, and at most offered an opportunity to consent or "opt-out" of data collection. Digital standards should clearly communicate and reinforce the organisation's data policy. For example, the United States Digital Service provides a concise and digestible privacy policy that applies to all digital services rendered.

Accessibility

This standard is about making sure everyone can equally access and use a digital service. For example, providing an instructional video without captions prevents those with permanent or temporary hearing disabilities from using its content. Digital service standards addressing accessibility should focus on **inclusive design,** which refers to a methodology of creating products, services or environments that are accessible regardless of age, disability or other factors. Digital services adopting this standard should ensure that they are compatible with **assistive technologies**, such as screen readers. Digital.gov, Smart Cities 4 All, and Accessibility Go! provide useful guidance for how accessibility can be introduced in digital services.

Equity

The pandemic illustrated the impact of the digital services design divide[9]. In response to the Covid-19 pandemic, critical public health services were provided remotely and digitally, leaving out many groups including the elderly, those who suffered from the digital divide, or those experiencing disabilities. The world's known digital divide problem was compounded by how services were designed and built in ways that excluded many types of users.

Digital government services must be issued in a balanced way that accounts for all types of people, lived experiences, and situations. For example, requiring a form of ID for a service may inappropriately exclude refugees and persons on the move, or providing a service exclusively online may limit people without internet access from using your service. Digital service standards that address equity should provide guidance for designing services that have a strong understanding of the environments your users may access the service in, and include options for paper-based or "analog" service delivery.

Security

There are several factors to consider when designing a secure service, and they vary with national contexts. Digital service standards should address authentication of users, encryption, resistance to exploitation, and include provisions for how the application is tested for vulnerabilities, as well as protocols for how these vulnerabilities will be addressed. These standards are critical for service delivery, and can be just as applicable to city staff as they are to private solution providers. It's important for local governments to have strong and transparent security standards in place, ensure they are well communicated in procurements, and receive confirmation that they are addressed by service providers.

Interoperability & open standards

Interoperability refers to the ability of different digital services to work together and communicate with one another. Typically, digital applications communicate through **application programming interfaces (APIs)**. This is particularly important for **data portability,** or the ability to transfer data across services. How does this translate to government services? Say for example, that a resident applies for housing assistance, and later applies for food benefits using two different platforms offered by the same government entity. If these platforms are not interoperable, then city staff may never be able to correlate the resident across these benefits. Interoperability and data portability are therefore critical for not only understanding residents' needs, but also correlating services, and minimising redundancies across the organisation.

Digital service standards should specify APIs that enable such connections between platforms. Access to APIs can be restricted by digital firms for security reasons, although some APIs are public and provided on an open source basis. Open source APIs are encouraged for new digital services entering an organisation's "ecosystem" of digital products. This helps avoid **vendor lock-in**, and can encourage competition in the digital services marketplace[10].

Data

How data is collected, exchanged and used underpins all digital services. Data has tremendous value for local governments that can analyse it for insights that improve service delivery, residents needs, and decision-making. Because of this, local governments should work towards maximising autonomy over data generated by digital services. This can be done through digital service standards that help identify the data and information services will use or create. Service standards should put appropriate legal, privacy and security measures in place, address access & control, data ownership, use and sharing, retention and overreach.

User-centred & responsive design

In order to build services that actually work for people, you must first understand the people who use your service and what they want to do. To do this, developers need to understand all aspects of your users' current experience. There can be multiple users of a service, not just the end-user or resident. Developers should consider everyone who is involved in the delivery of a service, including city staff, and intermediaries who help support access or use of that service. Understanding these stakeholders is typically part of the process of **user centred or "UX" design**. Digital service standards can make provisions for UX design, where developers are required to demonstrate how they have designed the service from the users' perspectives by doing user research, testing the service with prototypes, or analysing data to enhance their understanding of the problem.

End to end testing

Because digital services involve human behaviour, no successful service is designed in a vacuum. Therefore it's critical that developers of digital services test their product and iterate based on their findings. Often this is referred to as "beta" and "alpha" testing, where a product at varying stages of readiness is tested across users, studied, and improved. The 18F Testing Cookbook and GOV.UK Service Manual provide guidance for how to conduct such testing. Digital service standards can require or suggest that all digital services adopted by the government agency undergo this type of testing.

Measure performance

Measuring the performance of your service is important to understand what outcomes it is delivering. Digital service standards can require that developers report results to your stakeholders openly and often, in order to encourage rapid iteration and continuous improvement. To this end, it's often beneficial to establish **Key Performance Indicators (KPIs)** at the start of developing the service. These indicators can set important targets for things like how many users are targeted to use the service, how frequently the service is requested, or how many units of a service were delivered before and after implementation of a digital tool. Setting these KPIs and the intervals at which they should be measured during service development and delivery can help local governments evaluate how responsive their service is to people's needs.


FOR SALE
OGUN

Who should use digital service standards?

Digital services standards can be used by a variety of stakeholders, though they are intended primarily for anyone who is developing an application, web service, or other digital component of a public service. Developers can be both city staff, procured companies or third-party providers. External developers should follow digital service standards per their procurement contract with the local government entity. You can also check if companies under consideration for procurement already follow any existing digital service standards.

Digital service standards can be much more than rules for developers to follow, however. If they are made publicly accessible, such standards can increase trust in government by providing guide rails for technology co-creation and participation with the public. For example, the Australian Digital Transformation Agency supplements their digital standards with guidebooks for developers, training and mentoring programs, and access to communities of practice. Likewise, DIGI+ Taiwan, Taiwan's smart city program, invests heavily in hackathons and mentorship programs that support public development of government technology. In this way, technology development is seen not just as a necessity, but as a tool for educational and economic growth, as well as a means to re-imagine democratic participation. Digital service standards can increase transparency by explaining how digital services are built, and what values a local government has for the role digital services play in the community.

How to arrive at your digital service standards

So where do you begin? There are many ways for local governments to build digital service standards. Below are a few recommendations for how to get started.

- **Set up an advisory group** - Cities can get started by creating advisory groups for certain elements of the standard, or the standard as a whole. Advisory groups including local and regional experts can help shape the standards to reflect community perspectives.

- **Achieve leadership buy-in from a policy** - Alternatively, some cities may choose a policy instrument such as an administrative directive, ordinance or executive order to obtain leadership buy-in for the effort, prior to initiation.

- **Collect user feedback -** User feedback is critical for determining how well digital standards are working. This feedback can come from end users of a digital service, or from those who actively use the digital standard to develop tools and services. User feedback can be collected passively online where the standards are displayed, or after a transaction has been completed that uses a service.

- **Establish a means of governance** - Standards are most successful when effectively maintained. Standards should be reviewed on a regular basis (quarterly, bi-annually or annually) and revised by a dedicated committee based on performance and user feedback.

- **Create a community of practice** - Communities of practice bring together people with a vested interest in a subject area to collaborate, troubleshoot, and create new solutions. Local governments can create programming and events that bring together different stakeholders for digital service standards to collectively build new tools using the standards, or propose changes to them.

- **Promote the digital standards** - Make your digital standards more accessible by publishing the online and actively promoting them. Invite developers to use the standards through public events like hackathons or codeathons. Build training videos that help guide the public through your standards.

GOAL #2 Build your digital public infrastructure stack starting with payments, digital identity, and data exchange

Once you have standards in place for how you build digital services, the question then becomes– which services do you start with? Broadly, there are three major types of protocols that facilitate **digital public infrastructure**: digital identity, digital payments and data exchange[11]. These three protocols are typically required for most digital service transactions such as permitting, issuing licences, or providing records that often require validating a user's identity, enabling exchange of data across agencies and users, and finally authorising payments online. Collectively, they are referred to as a "stack" like a **software stack** where a group of independent programs and systems work together to accomplish a specific task. By prioritising these three protocols, local governments can set the stage for the successful development of an entire ecosystem of digital services in alignment with their community's unique needs.

BOX 2.1

Note about stateless groups, refugees and persons on the move

Accurate targeting is fundamental to successfully implementing social assistance programs, but in reality, reaching these beneficiaries can be extremely challenging. When people are involved in informal or agricultural jobs, they sometimes lack documentation making it difficult to accurately measure or verify potential recipients of important benefits. This lack of information can cause some undeserving beneficiaries to enter the program or leave other vulnerable households outside the safety net. Digital ID systems can potentially alleviate this lack of accurate data by facilitating improved record-keeping and generating administrative data on individuals in the country. Some populations, including refugees, migrants, and other 'stateless' groups, may be particularly challenging to reach or may inherently be excluded from specific ID systems on the basis of nationality/citizenship. In such cases, complementary ID systems may be necessary to reach these populations in order to facilitate access to social services and increase economic integration. For example, in Kenya, UNHCR has established a biometric database of refugees and asylum seekers that runs parallel to their national registration system.

However, the risk of technology failures leading to exclusion of eligible beneficiaries remains if access to biometric IDs is not universal or systems are not well implemented or managed. Issues around privacy and data misuse remains a major concern when data is collected and held centrally. Collusion could also occur by administrators or the state to exclude beneficiaries from certain groups, particularly if the ID system is linked to voting rights. Moreover, if beneficiaries are unable to navigate digital G2P (Government to People) payment systems, they may not be able to access their grants even when eligible, as seen in Jharkhand, India where it reduced the benefits for those who had not registered for an ID. Given that more vulnerable populations are often also those who have less access to knowledge on technology, this could mean the most vulnerable are particularly susceptible to exclusion when shifting to a digital mechanism.

BOX 2.2

Brazil's Digital Signature Platform

https://www-gov-br.translate.goog/pt-br/servicos/assinatura-eletronica?_x_tr_sl=pt&_x_tr_tl=en&_x_tr_hl=pt-BR&_x_tr_pto=wapp

In November 2020, the Federal Government of Brazil formalised the decree that establishes the bases for the use of digital signatures in the country, which have since been made valid and legally recognized for all types of digital transactions in interactions between people and private institutions with the public entities and between public bodies and entities. Among the documents that can be digitally signed by smartphones, are those related to the opening of companies and "startups" (innovative low-cost companies), in addition to the transfer of vehicles and proof of a real violator of car fines. To digitally sign, you must have an account on the platform, and you must previously perform an online facial biometrics. This service is offered by the Gov.br platform, which is a unified access channel to federal government services. To have access to these services, which range from consultation of certificates to benefits, it is necessary to register. The Gov.br platform is used, for example, for services of the Unified Health System (SUS), such as vaccination certificates, enrollment in the National High School Exam (Enem), consultation of the National Driver's License and retirement actions.

Digital identity

Identification systems collect and validate information to establish and validate a person's identity in the form of a credential, such as a passport or driver's licence. These credentials are then used to prove the holders' identity. **Digital identification** functions in the same manner, but as a digital alternative to physical forms of identification. Creating digital forms of identification can significantly improve the efficiency of services, but can also introduce potential human rights violations and accessibility risks for vulnerable populations if issues like privacy, the digital divide, and user-centred design are not well addressed.

When building a digital ID system, it is important to take note of the several models of digital identification and select the model most appropriate for your community. There are three main digital identity models: Centralised, Federated and Self-Sovereign. Centralised models are typically used by governments, where a centralised government entity issues ID credentials that users can then use across services. Under the Federated model, a handful of service providers issue credentials that can be used across specific pools of services. Finally, in the Self-Sovereign model individuals create and hold their own credentials, and all associated data. The Self-Sovereign model is the newest and most experimental of the three models, and is powered by recent innovations such as digital wallets and Blockchain.

According to McKinsey & Company, as of April 2020, 146 countries around the world launched digital identification systems, but only 46 leveraged those for digital public services[12]. This is in part due to challenges in scaling digital identification systems that result from a lack of interoperability, user-centred design, appropriate regulation, and an absence of trust with users. While the promise of digital identification is great, local governments must take an incremental approach towards addressing several key issues for a digital identity program to be successful:

1. **Centre the user in the design of the identification system -** Digital identification systems work best when developers fully understand who they are developing for. For example, the City of Baltimore recognized a need among vulnerable populations for an easy application that allowed for the sharing of credentials and documents required to obtain public services. The resulting "My Digital Data Locker" application was developed to help vulnerable populations maintain important documents safely and easily.

2. **Identify valuable use cases -** Users are more likely to adopt a digital identity system that actually solves their problems. Issue a survey, or host community dialogs to determine what services residents are struggling to use, and understand those transactions from a user's perspective. For example, obtaining permitting, requesting information about services or infrastructure, or applying for certain benefits can be easy ways to target and test the use of an ID system.

3. **Ensure interoperability -** An ID system is most successful if it is able to exchange data with other systems, databases, devices, and applications. Some jurisdictions have their own interoperability standards that local governments must follow. For example, the EU's eIDAS Regulation requires that all organisations delivering public digital services within an EU member state must recognize electronic identification from other EU member states. To get started, local governments can adopt international technical standards for identification systems[13].

4. **Create a positive user experience -** Good design is simple, clear and creates positive emotions after interacting with the service. Positive user experience is important to take into account because it enhances the likelihood of a service being adopted, and builds trust with communities. It is also important to set clear, enforceable boundaries about how the identification system can be used. For example, India's Aadhaar identification system was widely adopted across industries without significant regulation about how the identification system could be used. As a result, concerns grew about the possibilities of linking this identification system to all aspects of life, including banking, transportation and personal purchase behaviour[14].

5. **Build user trust -** Users will not use a service they do not trust. In order to increase adoption of an identification system, governments should prioritise security and privacy, and clearly communicate their approach with users. By adopting a privacy-by-design approach,[15] governments can bake privacy into the identification scheme. One successful approach towards building user trust is to provide users with transparency about what information is collected and shared about them. For example, Estonia provides citizens with a data-tracker tool that enables them to track when their information is requested or used.

BOX 2.3

Regulating India's Aadhaar Identification System

India's Aadhaar digital identity system is practically unequalled in its scale and implementation. Since the launch of the project in 2009, over 1.2 billion people have been registered in what is one of the world's most sophisticated forms of digital identity. Aadhar has been implemented in India, a country in which a large portion of the population has historically largely functioned outside of government registries: for example as of 2010, only 40% of the population was registered at birth, 3% payed income tax, and just 60 million (out of over 1 billion) possessed passports. Aadhar has essentially managed to create a singular database that, in many cases, has streamlined documentation for many people, particularly those who previously had no documentation, are now able to open bank accounts and access services.

Nevertheless, Aadhar is also a controversial system. With so much valuable information stored within the system, security risks cannot be overstated. The system has also provoked privacy concerns due to a lack of transparency at launch, regarding what data is collected and how it can be used. Other concerns emerged regarding the automation of benefits after one man reportedly died of starvation in 2017, after Aadhar's thumbprint authentication failed for family members seeking to purchase subsidised rations. In 2018, at least 15 deaths were publicly reported after people were denied basic resources when their identities could not be verified due to Aadhaar system errors. At the same time, Aadhar has been widely praised as contributing to better quality of life for many Indians, making services at large more accessible, and opening a wide range of new opportunities with increased governmental recognition.

BOX 2.4

Building Trust through Transparency: Estonia's Data Tracker Tool

https://e-estonia.com/data-tracker-build-citizen-trust/

Estonia is perhaps one of the best examples worldwide of the capacities of e-governance, with its homegrown X-Road system allowing ease of information sharing among and between government and residents. As is the case in all governments, information is constantly being exchanged between different bodies in Estonia. In Estonia however, with the X-Road system, such information sharing is often done with blockchain technology, allowing for clear records of information pathways. While blockchain technology does have major limitations, in the right hands it can allow for a high degree of traceability. Estonia has, however, brought data transparency even one step further. A data tracker tool has recently been launched that combines all information on records from the country's Population Record, Health Insurance Fund, the Estonian Unemployment Insurance Fund, and the Social Insurance Board in one place. While other bodies have yet to be included in this platform, citizens are now able to easily access records of when and to where their personal data has been shared. While other bodies also have their own individual records of their data sharing, this effort in any case represents a strong move towards greater transparency, with much more information to be found in one place, granted in an already very advanced environment. Perhaps worldwide, with the increased integration of improved e-services and blockchain technology, similar data tracker tools will become increasingly commonplace.

BOX 2.5

Review: Blockchain's role in digital identification

The blockchain offers great potential for the management of identities, bypassing more traditional systems. While in many cases the sheer logistics of producing and accessing physical identity documents can be difficult, especially for the needs of populations like the homeless and refugees, blockchain technology presents an alternative when documents are not easy to handle. In the case of Austin, Texas a pilot project called the MyPass Initiative, driven in partnership between the City of Austin, its county's medical services, and the University of Texas, is providing blockchain-based identity to homeless residents of the city, allowing them to access services and access and share records while lacking physical documents. For such populations, lacking physical addresses and often unable to hold onto or obtain things like medical records or driver's licences, the blockchain, which allows traceable communication with various databases, presents a possible advantage.

This technology is also potentially quite helpful for wider populations as well, however: in Zug, Switzerland blockchain based identities were piloted in voting initiatives. Nevertheless, there are privacy concerns that must be taken into account, as it can be expected that many end users are not particularly technically literate, potentially prone to the misuse of their information. The blockchain as a concept, as well, also faces criticism as it is a new technology largely associated with speculative and potentially questionable industries such as cryptocurrencies and the NFT market.

Data exchange

All digital services are powered by data being exchanged between systems and users. Therefore, it is important for local governments who are building digital services, or procuring to clearly identify protocols and security measures for how data is exchanged across systems, platforms and users. The topic of data exchange for enterprise systems is vast, and there are several resources and guidance for establishing robust data transfer systems. For the purpose of this playbook, we will focus on three key areas that municipal governments should be aware of when establishing digital services: **metadata** (information that describes data), secure transfer (protocols for how data is securely exchanged), and transfer method (how data is exchanged).

1. **Metadata -** Metadata refers to information associated with a dataset that provides a common way of structuring and understanding data. Establishing metadata standards is considered a best practice for ensuring that data can be uniformly and easily read, understood and used when it is exchanged across systems and users.

2. **Secure transfer -** Data must be securely transferred across platforms. Local governments should check to see if there are any national standards for data exchange they must follow. For example, in the United States the federal government has adopted the secure HTTPS-Only standard, where data is encrypted across the exchange.

3. **Transfer method** - There are a variety of ways that data can be exchanged across services, and which one is selected varies according to the complexity of the data, frequency of transfer, size of the dataset, and organisational considerations. Some common transfer methods include Application Programming Interfaces (APIs), Extract Transform and Load (ETLs), file transfer, and data streaming. Harvard University's Data Exchange Methods and Considerations provides useful guidance for understanding and selecting data transfer methods.

Digital payments

Finally, digital services must allow for easy and secure transfer of payments. The CoVID-19 pandemic greatly increased the volume of digital transactions, as the digital economy grew in response to global lockdowns and restrictions on in-person gatherings[16]. This introduced opportunities for financial inclusion and to prioritise women in the realisation of financial equity. According to the UN's Better than Cash Alliance[17], digital payments are defined as "the transfer of value from one payment account to another using a digital device such as a mobile phone, POS (Point of Sale) device, computer, or digital channel of communications such as mobile wireless data or SWIFT (Society for the Worldwide Interbank Financial Telecommunication). Digital payments include those made with bank transfers, mobile money, and payment cards including credit, debit and prepaid cards.

When developed inclusively, digital payments are known to enhance inclusive economic participation. For local governments, adopting and encouraging digital payments can lead to several known benefits including cost savings, enhanced transparency and security. Furthermore, because digital payments are widely accessible they are also an instrument of financial inclusion[18], and can encourage women's participation in the economy, by giving them more control over their finances[19]. Governments can invest in digital payments by developing systems that enable direct payment from users to government (Person to government or P2G payments), or by unlocking opportunities for small businesses to adopt digital payment systems (Person to bank or P2B payments)[20].

UN Principles for Responsible Digital Payments

The UN recognizes the digitization of payments as a means to reach financial equality and advance the SDGs[21]. The UN Principles for Responsible Digital Payments cover key actions that can yield more inclusive digital payment systems. These principles can be used by governments to guide their responsible decision-making and investments in the digitization of payments. Below is a brief summary of the principles.

- **Treat users fairly -** According to the Better than Cash Alliance, the next billion digital payment users will represent underserved and vulnerable communities. This principle refers to how governments and companies can ensure best practices in digital payment design and implementation so that digital payments are unbiased and accessible.

- **Ensure funds are protected and accessible -** In order to be effective, digital payments must be secure and reliable. Governments can build trust with users by giving them transparency and control of being able to view, access, and use funds on demand. However, doing so requires protecting these transactions from phishing, fraud, and unauthorised use.

- **Prioritise women -** Women often suffer from systemic and organisational biases that exclude them from participating in the economy. In order to expand the benefits of digital payments, women's lived experiences must be prioritised in the design and delivery of digital payment systems. Governments can do this by building strategic partnerships that enhance women's participation, and closely monitor the impact emerging technologies have on inclusivity.

- **Safeguard client data -** Like so many smart city technologies, digital payments are generating volumes of new data. This data has the potential to provide insights that can positively shape the design of digital payment services. However, increased data also increases the risk of misuse. To effectively steward client data, governments must include clauses in their service-level agreements with digital payments providers that protect client data, and set standards for data ownership, privacy, and protection.

- **Design for individuals -** To create a world where digital payments enhance everyone's livelihoods, a deep understanding of users' needs, preferences, and capabilities is essential. Digital payments must be responsive to lived experiences of users, and governments can support this by building grassroots partnerships with civil society to better understand needs, and regulating service design and delivery to be more responsive.

- **Be transparent, particularly on pricing -** To ensure an inclusive future for digital payments, governments must communicate information about these systems, how they work, and where users can obtain assistance using them. From a regulatory standpoint, governments can introduce rules about transparency in service-level agreements or procurements for digital payment services.

- **Provide user choice through interoperability -** Siloed digital payment models, where users must independently pay fees for each provider, or systems are intentionally not interoperable, limits inclusivity and participation. This principle advocates that companies should collaborate with competitors to invest in common infrastructure requirements for digital payments, and that governments can also invest in shared infrastructure to reduce costs and increase access to digital payments at the last mile.

- **Make recourse clear, quick and responsive -** Increased use of digital payments has also increased the number of grievances, and therefore the need for robust recourse procedures. Recourse processes should be clearly defined and accessible to users, making specific provisions for women and vulnerable groups. These requirements can be baked into agreements with service providers. Additionally, users should be able to easily provide feedback and complaints, and these grievances should be tracked and responded to by service providers.

- **Champion value chain accountability -** There are an increasing number of actors in the digital payments space, including third party providers and backend users. Taking responsibility across the value chain means establishing clear oversight over digital payment systems, and building a shared understanding of the responsibilities of each actor in the value chain.

BOX 2.6

Building Blocks - Leveraging blockchain for humanitarian assistance

https://innovation.wfp.org/project/building-blocks

Building Blocks Network is the world's largest implementation of blockchain technology for humanitarian assistance; currently assisting 1 million people in Bangladesh and Jordan, enabling them to securely access and receive multiple forms of assistance from different organisations via one access point.

The use of this type of infrastructure has multiple benefits. First, the network is neutral without a hierarchy of ownership or central control. All members of the WFP organisations are 100 percent equal co-owners, co-operators, and co-governors of the network and all members play an equal role in its upkeep. Second, the project is a collection of blockchain nodes which are computer servers independently operated by each participating organisation. This means that every piece of information should be validated with the other servers, making it challenging to edit or delete information. Although this is not a "hack proof" system, it has demonstrated that it is less vulnerable than other commonly used databases. Third, contrary to financial institutions used before, no sensitive information, such as names, dates of birth, or biometrics, are stored anywhere on Building Blocks. The system uses anonymous identifiers to ensure the privacy and security of people served. Lastly, the technical blockchain infrastructure to operate the network is based on open-source software and is freely accessible to participating organisations. According to a study made by the University of Geneva this infrastructure reduced local banking fees by more than 90% and reduced financial risk by not having to deposit money upfront to local financial institutions.

BOX 2.7

Vietnam's Consumer Protection Directive

In 2019, the Vietnamese government issued a new draft directive specifically targeting increasing consumer protection in what remains, in many places, the rather murky world of online personal data. This legislation applies various conditions to the collection of personal data, requiring for instance, consent from users and high levels of data protection in recipient countries before data can be transferred out of Vietnam. Designed to target abuses in the world of big tech, both in and outside Vietnam, specific monetary fines have been planned for failures to de-identify/anonymise consumers' personal data.

The government has also planned to take on a stronger role in enforcing and monitoring this field, with the creation of a "personal protection committee" in the country. While the EU's GDPR Regulation is perhaps the most widely known data protection legislation in the world today, countries in very different regions and with very different political contexts, such as Vietnam, are also increasingly implementing controls in this previously under regulated area.

BOX 2.8

WFP's blockchain-based cash transfers in Bangladesh

https://medium.com/world-food-programme-insight/how-blockchain-is-helping-wfps-fight-against-covid-19-in-bangladesh-d2b466a8becf

The World Food Program (WFP) uses blockchain technology to create a shared database of humanitarian cash assistance programs that collect disbursements from multiple agencies as a lump sum, using QR technology to facilitate transactions. At the foundation of the program is a shared database of beneficiary information – including which programs they are receiving benefits from – that is stored and encrypted using blockchain technology. These "blocks" are available to humanitarian organisations as a common resource. These blockchain-enabled QR codes are scannable not only by the organisations disbursing relief, but also by retailers (e.g., grocers) selling food and other necessities, enabling an interoperable user experience at the point of service.

Operational since 2017, the project provides recipients with a blockchain-based e-wallet to make cash transfers faster, cheaper and more secure, allowing WFP to transact directly with recipients without the need for banks or other financial institutions. Record of the transaction is updated in real-time on the blockchain, enabling organisations across the humanitarian sector to ensure individuals are receiving the right assistance, at the right time. This helps improve the coordination, optimization and transparency of humanitarian response between organisations. Additionally, individuals are issued an encrypted ID or code number to distinguish them from others, without revealing their true identities, key for security and privacy reasons. A digital QR code is issued allowing people to collect assistance without having to handle potentially contagious devices. That assistance is stored in a digital account to use at outlets within the camp. Once the person decides what items they want to purchase, the money is sent to the local retailers contracted to run those outlets, helping spur the sustainable development of the community while boosting the local economy.

Digital government services powered by the digital public infrastructure stack

With digital identity, data exchange protocols, and digital payments in place – what kind of digital services are made possible? There are a wealth of possibilities, and best practices associated with each. This section covers what types of digital services can be built off of the digital government stack, and important considerations for their development.

BOX 2.9

Data privacy and human rights considerations for the Digital Public Infrastructure Stack

https://www.cambridge.org/core/journals/data-and-policy/article/rethinking-digital-identity-for-postcovid19-societies-data-privacy-and-human-rights-considerations/0B9A65B889C341CF535E804256C2816A

It is essential in an era in which digital public infrastructure continues to expand at an unprecedented rate, that projects take data privacy and human rights considerations firmly into account. This is particularly relevant in the context of the COVID-19 pandemic, and its push for at once decentralised and new forms of digital identity. While conventional forms of identification are prone to many forms of weaknesses, newer and often untested forms are a particular area of concern in this regard. Breaches of personal information and its collection and distribution without personal consent pose major risks to human rights. In the EU, data protection impact assessments are often required in many cases, essentially gauging risks concerned and outlining measures taken in response.

Nevertheless, legal frameworks more often than not are behind the times, with little either codified or enforced in the protection of data. Similarly, in many cases, it is important to consider the "digital gap" in populations as digital identities become more important, as older or more marginalised populations, for instance, will likely have more trouble accessing services and noting problems. It is also important that new systems should have clear terms of accountability and adjudication of grievances, as with a "black box" of information, systems can lose touch with the people they serve. It is therefore very important that systems be designed based on relevant impact assessments, with input from all the stakeholders concerned, and that they be accessible to adjustment, oversight, and criticism in their implementation.

Tax and public finance

The pandemic increased public expectations for accessible and user-friendly digital services. **Digitalising tax administration,** while challenging, has the potential to deliver major benefits for society, reduce inequalities, and increase revenue that can further support the SDGs. For governments, benefits include higher revenue from increased taxpayer compliance, lower administrative costs, increased transparency and accountability, quality data for decision-making, and a broader tax base from small businesses particularly in developing contexts.

The Better than Cash Alliance has published a guidebook[22] for governments seeking to digitalise their tax administration processes. The guidebook provides 10 principles for digitalisation, and documents best practises from countries that have successfully implemented tax digitalisation, such as Rwanda, Mexico and Indonesia. By streamlining tax collection, some governments like Mexico have seen as much as a 48% increase in revenue collection[23]. Governments can also use tax digitalization to bring small businesses into the formal economy, thereby increasing overall tax revenue. This is particularly relevant for cities and countries with significant informal economies.

Public benefits

The Digital Public Infrastructure stack creates opportunities for local and national governments alike to collect accurate information about those they serve. As a result, public benefits can be more appropriately allocated, avoiding the common inclusion errors (when undeserving beneficiaries access benefits) and exclusion errors (when eligible beneficiaries are excluded from or denied benefits). Public benefits can include unconditional and conditional payments for welfare and benefit programs like social pensions, retirement pensions, social security, healthcare, education assistance, food benefits, and energy or water assistance. Too often, the most vulnerable are left behind because they are traditionally harder to reach. For example, according to the World Bank's ASPIRE database, only 22 percent of the poorest households in sub-Saharan Africa receive any form of social assistance.

Digitisation of public benefits allocation typically uses automated systems to tie benefits eligibility with a beneficiary's digital identity. Automating this process can close the error gap, and increase the reach of benefits allocation. However, governments must be cautious when digitising public benefits allocation as technical

BOX 2.10

Mexico's Tax Policy and Administration Reform

For governments, digitalization can lead to cost savings by improving administrative efficiency and operational productivity, increasing net revenue. Mexico has been among the forerunners in tax digitalization. With a process that started in 1980 this country is now one of the most advanced digital tax administration systems among the world's emerging economies. Over several decades, Mexico's impressive tax digitalization journey has been driven forward by the Tax Administration Service (SAT), the national entity responsible for collecting federal taxes. These taxes, Corporate income tax (CIT) and personal income tax (PIT), and value added tax (VAT) represent around 80% of the total revenue collected nationally each year in Mexico. Through sound strategic decision making, far-sighted reform with robust implementation, and ongoing investment, Mexico has delivered impressive results:

- Increase its overall tax revenue and social security by about 95% from 2010 to 2016.
- Tax-to-GDP ratio rose from 12,6% to 16,2% between 2012 and 2017.
- Total tax evasion fell from 35,7% to 16,1% in the years 2010 and 2016.
- SAT reduced the cost of tax collection by 57% between 2006 and 2018.
- Revenue generated by audits increased by 117% over the last five years.
- Increased the tax base by around 150%.

SAT's digitising tax payments and related processes can raise an additional USD 300 billion in government revenues annually in emerging and developing countries. This is equivalent to almost one-third of the USD 1 trillion funding gap, which has put the Sustainable Development Goals at severe risk.

errors can be costly, or possibly even fatal[24]. Digitisation must include clear and accessible channels for recourse, training for system administrators, and should always "keep a human in the loop," by using automation as a supplement to, rather than a replacement for public servants.

Asset tracking

Establishing an inventory of public assets, particularly infrastructure like streetlights, sewer mains, and traffic lights can be a challenge for many local governments, particularly those operating in informal or developing contexts. Emerging sensor and **Internet of Things (IoT) technologies** have created opportunities for better asset tracking by outfitting public infrastructure with sensors that can provide real-time diagnostic information about the status of an asset. This has led to a surge of platform tools allowing city officials to track and manage assets in real time. Such combination of different technological assets and their information in one place, aimed at mirroring physical urban processes and improving operational efficiency on urban management, characterise what has been widely referred to as **digital twin**.

To build a digital twin, asset data is collected in a variety of manual ways including laser scanners, LiDAR, drones, sensors, and cameras on surface vehicles. Manually collected data is then uploaded into a platform and correlated with other public or proprietary data sets such as climate, air quality or other environmental data. Data collection at this scale is referred to as **big data**, and demands a high capacity of storage and processing at high speeds. Local governments seeking to build a digital twin, should consider costs associated with maintaining IoT infrastructure, and "re-scanning" the environment periodically to update data. They should also work to address the privacy risks posed by environmental scanning, by automatically blurring personally identifiable data such as people's faces or licence plates. Digital twins are also under development by non-state or commercial actors for proprietary purposes, therefore local governments seeking to use this technology should ensure they have adequate contract language in place to guarantee their ability to access, control, and manage the data assets free of charge. This can include the use of an acceptable use licensing clause in a service-level agreement or contract, for example, where the data generated by a digital twin is owned by the municipality and licensed to third parties.

Land titling

Digitising a land registry can create more reliable property records, increase transparency of property ownership and information and support a more efficient property transfer process. Paper-based land titling systems sometimes risk damage, fraud and theft with dire consequences for property owners and farmers. The threats of climate change and natural disasters further impact paper-based archives and property records. For example, the 2010 earthquake in Haiti destroyed nearly all of Port-au-Prince's municipal archives, resulting in the destruction of property records that lead to ongoing disputes about property ownership today[25]. Digital documentation is not invulnerable to risks, however. Security processes for digital archives require continued investment and protection from an evolving landscape of cyber threats.

Some governments, particularly those with significant agricultural sectors, have prioritised land titling as part of their digital transformation process. For example, India's Digital India Land Records Modernisation Programme (DILRMP), plans to create a unique identification for every land parcel in the country by Spring 2022. Other governments, including Bermuda, Georgia, Ghana, India and Honduras are initiating blockchain-based land registries, where property information is stored and accessed on the **blockchain**.

Before making the transition to digital land registries, policy makers must develop a robust legal framework for the technology, and assess technological capabilities as well as organisational capacity factors. The World Bank has published a guidebook for digitisation of property records[26].

BOX 2.11

Use cases leveraging blockchain for land registries

While blockchain technology is often complex and energy inefficient, it can present clear advantages to the management of land tenure, allowing, at once, for gains in transparency, accuracy, and efficiency in land registries. In the Republic of Georgia, the country's National Agency of the Public Registry (NAPR) has partnered with the company Bitfury to create a blockchain-based land registry. This was done to combat many of the problems common to land registries around the world: risks of corruption (with details potentially being changed by corrupt officials) and opacity in access to information and administrative and financial barriers to gaining formal registration. With the blockchain, land registration can be done much faster, and in a theoretically publicly accessible manner. The blockchain system can also more easily accommodate different property rights regimes (allowing for easier and more varied exchanges between individuals), and step in when governments have limited capacities. The positive externalities of improved land registration are potentially immense, limiting various forms of insecurity and allowing increased access to services of all kinds. In Georgia's case, aside from producing a better (and less corruptible) register, land registration also became far easier, taking on average one day to complete (as opposed to 15.2 and 39 days in the United States and Germany, respectively) and costing only an approximate 0.1% of property value. While the blockchain isn't necessarily essential for building such an improved system, it can provide one means of facing down problems common to land registration.

Civic participation and voting

The Digital Public Infrastructure stack also unlocks opportunities for digital forms of public participation, including voting, which relies heavily on a robust and secure digital identity system. Making civic participation digital can increase public participation, as citizens can contribute to democratic processes from the convenience of their home, and at their own schedule. Provided a municipal government has a strong strategy to combat the digital divide, and can dedicate resources to marketing and communications, digital public participation systems can increase civic engagement levels. Allowing simple, low-tech citizen verification continues to be a valid solution, and non-technological or paper-based solutions should remain in effect to ensure accessibility and accuracy.

Perhaps the most popular example of virtual public participation is the E-estonia platform, where 99% of government services are offered online, residents can pay taxes, receive prescriptions, and bank all under a single e-residency identification which is accessible transnationally. E-estonia offers a toolkit to familiarise participants with the platform. Additionally, *Co-creation and Collaboration in Smart Cities: A playbook for local and regional governments* provides an extensive overview of digital public participation tools and best practices.

Procurement

Digitalisation of public procurement can introduce new opportunities for third party monitoring, transparency, and accountability in the procurement process. They can also streamline administration and expand opportunities for small and minority owned businesses to compete for government contracts, in addition to improving the efficiency of public spending. Following CoVID-19 local and national governments alike have had to address how to redesign and digitise **source-to-pay** systems in order to be more responsive, automated, and accessible. Emerging technologies like robotic process automation, machine learning and natural language processing are currently being developed and evaluated for the role they can play in redefining procurement processes to be more agile and transparent[27].

However, procurement processes are complex regulatory frameworks with multiple requirements and a variety of users. Therefore the digitalization of procurement processes can be challenging and nuanced, requiring that the entire process be transformed end-to-end, so that all users in the procurement process operate in a fully digital, and interoperable environment. For example, Chile launched ChileCompra, an electronic procurement platform in 1999. Since then, the Chilean government has focused on improving the platform, and trained thousands of government employees and private partners. In 2017 a review by OECD found the number of businesses transacting through ChileCompra increased 180% from 2010 to 2015[28].

BOX 2.12

ChileCompra procurement reporting platform

https://www.chilecompra.cl/wp-content/uploads/2016/11/strategic-plan-public-procurement-system-2002-2004-2.pdf

Chile's information and support for procurement professionals was sparse and varied, with procurement regulations incoherent and dispersed. The manual nature of procurement meant an amount of USD 12 million in newspaper advertising. The low uptake of e-procurement and the resulting lack of publicly available information also resulted in a growing sense that government spending was not transparent or accountable. At the time, public procurement accounted for USD 7 billion of public spending annually through more than 1.4 million transactions. In 2020, ChileCompra's role as the central purchasing agency in Chile was realigned to focus on the implementation of collaborative procurement instruments for the benefit of contracting authorities. Its main duties are to:

- Provide support to public entities in carrying out procurement processes;
- Implement, operate and maintain the e-procurement system, allowing public entities to conduct online procurement operations;
- Manage the registry of suppliers;
- Purchase goods and services on behalf of one or more public entities; and
- Implement and manage FAs.

Contracting authorities in Chile are obliged to use ChileCompra, while other entities such as municipalities, can voluntarily participate should they wish to. Increasing the coverage and use lead to a greater potential for generating price savings and process savings through consolidation of demand.

According to ChileCompra, in 2017 the savings generated from the use amounted to USD 1 410 million. The OECD's 2017 review of FAs in Chile analysed the number of businesses transacting through ChileCompra FAs and identified an increase of 180% from 2010 to 2015. These objectives can often conflict with the policy objective of an inclusive and open approach that encourages broad participation in FAs by Chilean suppliers of all sizes. Instead, distributing revenue across a large number of suppliers avoids the concentration of spend in a small number of large companies, and spreads the economic benefits of government spending more broadly.

GOAL #3 Build capacity and governance for digital public infrastructure

Successfully building digital public infrastructure requires restructuring organisational capacity, digital skills training, and building supportive external partnerships with civil society, private companies and NGOs. Collectively, these activities form the 'governance' of digital transformation. Governments looking to digitise must choose between developing solutions in-house, or procuring solutions. When procuring external solutions, local governments should take care to bake legal or policy requirements for privacy and security at a minimum into their requests for proposals (RFPs), and consider including best practices for user-centred design, and interoperability.

In order to build capacity within the organisation, governments must invest in upskilling existing staff, and creating competitive conditions to hire new talent. Digital capacity training programs can focus on several topics including software, UX design, agile development, digital government services and digital tools, design thinking, coding, digital human rights and inclusion and cybersecurity. To facilitate internal capacity building, four main approaches are most widely used:

- **Demand-driven** - Offer training and capacity building services based on listening tours, and facilitated discussions with city staff.
- **Needs-based** - Deliver training and capacity building services based on a capacity needs assessment.
- **Holistic** - Design policies that incentivise or require training, and provide the necessary tools and resources for compliance.
- **External** - Work with an NGO or external certification program that requires certain benchmarks to be met and can provide resources and training to your local government to achieve programmatic goals.

Governing digital public infrastructure requires introducing controls, regulation, and increasing opportunities for transparency and public oversight. Approaches to digital governance include developing open standards, ensuring data ownership and interoperability, and introducing procurement standards that control for desired outcomes of digital services. These approaches and best practices are outlined in detail in Section 02 of *Co-creation and Collaboration in Smart Cities: A playbook for local and regional governments*.

Limits and risks of digitisation

Digitisation is not a silver bullet, and often digitisation projects are delayed, over budget, or fail to deliver expected results. Within public service, the digitisation process commonly faces some cultural resistance among public agents, due to reluctance to change existing systems and processes. Digitisation projects also carry significant risks of exclusion, for example for women, rural populations with limited internet access, or other vulnerable communities. Therefore, the decision to undergo digital transformation should be weighed carefully, taking into account several key issues.

- **Digitisation can exacerbate dysfunctional processes -** Digitisation will not be successful if it merely replaces a poorly-designed process. Instead digitisation represents an opportunity to redesign a process so that it is more functional, efficient and responsive. Governments embarking on digital transformation should conduct an analysis of the systems they seek to replace, survey internal staff, and collect feedback from end users to inform the redesign process.
- **Digitisation can introduce significant risks to privacy, security, and exclude vulnerable groups -** There is a growing body of evidence that digital identification and digital payments can create privacy and security vulnerabilities for users and introduce risks to vulnerable populations[29]. Governments should assess these risks and introduce the necessary policy, recourse processes, and legal protections in advance of deploying digital services.
- **Digitisation requires resilient physical infrastructure -** Digital infrastructure relies on basic physical infrastructure such as electricity, internet connectivity or mobile phone penetration. When designing digital services from a user-centric perspective, developers should consider whether the basic needs of these users are met. Digital services must also be resilient to challenges posed by climate change and natural disasters, and consider how to bake such resilience into their design.
- **Adoption of digital services requires digital literacy and universal internet access -** Digital literacy of both users and service providers is critical to the success of any digital transformation effort. Governments that are transitioning to digital services must also invest in addressing the digital divide, and digital literacy programs for both residents and city staff that ensure digital services are inclusive and accessible. It is crucial to maintain non-digital forms of access to government processes.
- **Successful digitalisation rests on multi-sector support and sustainable governance -** No organisation can complete a digital transformation journey alone. Governments should explore resources offered by NGOs, evaluate the potential offered by public private partnerships (P3s) and incorporate the expertise and perspectives of civil society and academic institutions in the process of their digital transformation.

03

ACTIVITY 6:

Create a data governance framework that sets standards and responsibilities for effectiveness, accountability and inclusivity

SDG 16, 16.6.
New Urban Agenda 157, 158, 159

Core Values

1 Public data architecture

Value 1: Users should be placed at the centre of public data architecture that gives individuals more autonomy over governments use of sensitive personal information.

2 Public consent

Value 2: Data collected indiscriminately and without public consent presents human rights risks.

3 Accessibility to data collected

Value 3: Local governments should make provisions to own data collected or generated by technologies and make non-sensitive data assets accessible to the public by convenient means.

4 Participatory public process

Value 4: Data collection should be based on public interests defined through participatory public processes.

Introduction

Data is the lifeblood of smart cities and what we choose to collect data about, and how we collect it shapes our values as communities. Because data underpins so many smart city applications, having policies that govern how data is managed and protected is critical for cities to thrive in the 21st century. **Data governance** refers to the collection of policies, processes, and standards that ensure the quality, integrity, security, availability, usability, and accessibility of a city's data assets while respecting residents' rights to privacy.

Data has tremendous value to cities who can harness it to develop evidence-based policy and data-informed programming that addresses the real needs of residents. Emerging smart city technologies like smart streetlights, digital twin applications and Internet of Things deployments also collect new data sets that cities must evaluate for their potential to improve quality of life for residents. Having a shared, standard process for managing the data that flows through the organisation is important for several key functions of city government:

- **Developing and measuring services** - Data is key to evaluating the performance of a city's programs and policies. Data governance helps to standardise how data is used to build better services and measure their effectiveness.
- **Evidence-based policymaking** - Policies built on evidence require that data has integrity, meaning that it is clean, searchable and usable.
- **Protecting privacy across digital services** - Effective and responsible data management is needed to ensure the protection of resident privacy, and the privacy of anyone using digital public services or infrastructure.
- **Understanding your community and environment** - Data creates opportunities to analyse information about your community and environment, and collect information from residents through meaningful consent. Policies can set standards for how data is collected, analysed and used.
- **Procuring useful and ethical solutions** - When municipalities purchase technology that collects data or generates new data, data governance policies establish rules for data ownership, licensing and transparency requirements.

However, without clear standards for data management, local governments risk exposing themselves to expensive data subscriptions, creating data silos, violating privacy laws, and producing less efficient, and more expensive workstreams. Cities face several common challenges on the journey towards data governance:

- Lack of data privacy legislation at the national or regional level.
- Losing control of data in procurements.
- Lack of awareness of privacy and how data is used and generated by emerging technology.
- Lack of infrastructure.
- Lack of a responsibility matrix.
- Challenges negotiating data sharing agreements.
- Bias in methods of data collection and analysis.

In the face of these fundamental challenges, what can city governments do to harVower of data and data-driven technology? The process of collecting, cleaning, integrating, and analysing data requires capacity and capital investment, organisational culture change, interagency collaboration and long-range vision.

Fortunately, there are tremendous examples of best practices from cities who have developed effective strategies and policies to guide the development of more open, data-driven city government.

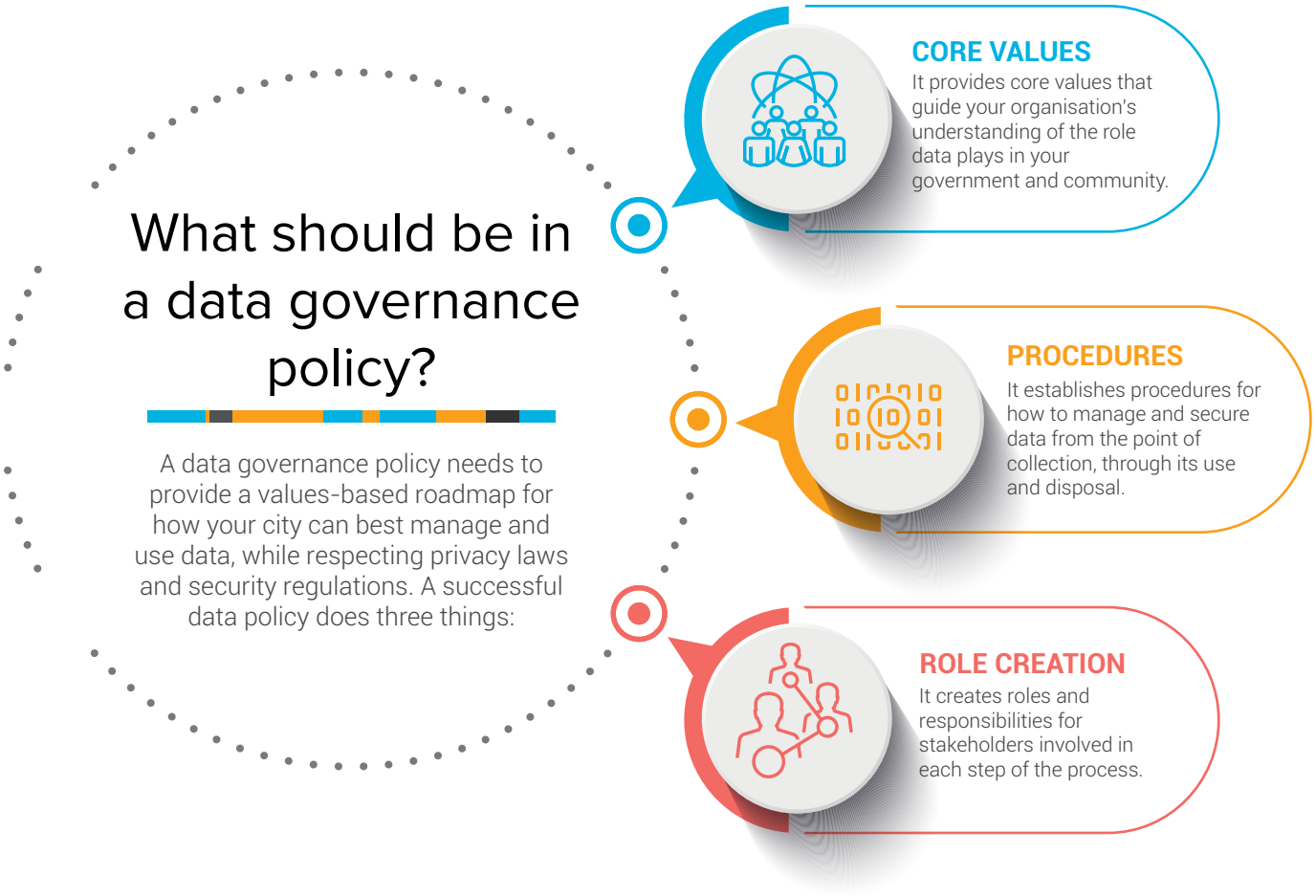
This section reviews those best practices and makes four main recommendations:

1. **Create a data governance directive** or policy with leadership and stakeholder buy-in that outlines core values for data governance, and can be used to justify investment.

2. **Build a program to train city departments on your data governance directive** and implement a data governance policy.

3. **Evaluate, test, and build public and internal data platforms** that operationalize your policies.

4. **Identify opportunities to create new participatory processes involving data** that build digital literacy and create new feedback loops.



GOAL #1 Create a data governance policy, executive order, ordinance, or directive that sets the rules for how your local government manages, uses, and secures data, including operational processes

Data governance policies vary depending on context, available technology, and community values. Local governments should understand what national policies and other frameworks are in place which support their city's data governance aspirations. Establishing ownership over its data assets is paramount for a municipality's ability to protect public interest in the design and development of digital services. Therefore, data governance policies should clearly indicate how the organisation will treat data ownership in its procurements.

Below is a brief overview of each of the key components of a data governance policy for local government.

- **Principles or core values -** Data can play many roles in a government and by highlighting your organisation's core values, your city government sends a strong message about what matters most. Cities can champion themes such as data-informed decision-making, data integrity, ethical use of data, privacy, and **data sovereignty**. By including principles in your policy, you are channelling the use of data by your organisation towards a purpose. For example, the City of San Antonio's Principles of Data Informed Government outline key values for their data governance policies and programs.

- **Roles and responsibilities -** Your policy should cover specific roles within your organisation for carrying out data governance responsibilities. These roles can include IT Roles and Business roles, such as **Data Stewards**, or Data Owners. Each role should have a designated purpose and responsibility, and these must be clearly defined in your policy.

- **Data classification -** Different types of data should be handled according to different procedures. Therefore it is important that your data policy provides criteria for classifying data into specific categories, and outlining procedures for each. Common data classifications include open data, agency sensitive data, and confidential data.

- **Privacy -** How an organisation will ensure data privacy is fundamental to a data governance policy. A data governance policy should provide transparency to the public regarding what type of data is collected by the organisation. Generally, data collection should be minimised to what is adequate, relevant, and necessary to meet a clearly specified public need or interest. **Personally identifying information (PII)** should not be collected without consent. Policies should be transparent about whether data collected by the organisation can be monetised or sold to third parties. Vendors who are awarded contracts with the municipality or handle data on their behalf should be required to comply with the data privacy policy.

- **Security -** Security is a major concern among local governments, and security standards should be addressed by a governance policy. Sometimes, security standards are established at the national level, and local governments should take care to specify what standards they adhere to. Policies should address how data will be securely stored, protocols in the event of a breach, data destruction, and roles and responsibilities.

- **Data sharing -** Data is not static, and can be considered as a service that is provided to external groups such as civil society or academic institutions. The policy should outline key stakeholders for the municipality's data, and specify protocols for sharing data with each. If there are data sharing agreements in place, the policy should point to those agreements where appropriate.

- **KPIs, and standards for operations -** Guidelines for data collected about performance measures for the organisation can also be captured in a data policy document. If the directive is followed by city staff, it represents an opportunity to streamline how different city departments collect data to monitor their own performance.

- **Procurement guidelines -** When cities procure new technologies, products, systems or software, they must ensure that any data collected or generated by these solutions complies with the data governance policy. Specifically, issues such as data ownership, interoperability and data security can be addressed as they relate to public procurements.

BOX 3.1

City of Cape Town: Unlocking data for collaboration using a data strategy

https://admindatahandbook.mit.edu/book/v1.0-rc5/cct.html (Chapter 13)

The City of Cape Town represents one of Africa's best examples of digital transformation, launching its own data strategy as well as establishing a data science unit, a body specifically tasked with facilitating greater data sharing, enhanced tools for analysis, and advanced analytics. This policy was designed with, and continues to be monitored and improved by, a partnership with the University of California, Santa Barbara and the Abdul Latif Jameel Poverty Action Lab.

The emphasis on building an effective data strategy in Cape Town came about from a need for collaboration and information sharing, which was previously done on an ad hoc basis, or based on individual relationships. Cape Town's advanced data capabilities have already helped it in notable ways, from painting a cohesive picture of water supply and usage in the city during its recent multi-year drought, to tracking community spreading of COVID-19 more recently. The data collected is also freely available to be used in research and has contributed to better informed policymaking.

Cape Town can serve as an effective example for other cities interested in developing a data strategy, particularly essential today in Sub Saharan Africa and small and medium-sized cities of the world where local capacities can lack the capacity or resources for such an initiative. However, Cape Town's system does face challenges with interoperability, accessibility, and privacy concerns that have yet to be resolved.

- **Guidelines for emerging technologies: AI, automated decision-making, IoT -** Some cities have introduced guidelines for emerging technologies such as artificial intelligence. These guidelines pertain primarily to city departments that procure solutions involving these technologies or develop them, and private sector companies that provide them to the city. As this is an emerging topic, examples of these guidelines vary, but tend to focus on reducing potential bias when data is used for automated analyses. For example, New York City has issued a strategy for Internet of Things technology.

- **Data & community engagement -** Data policies can also focus on how data is leveraged as both a service and tool for the community. Policies can highlight specific programs, designate advisory communities for data related issues, or outline roles and responsibilities that the community has when it comes to data governance.

Who can use a data governance policy?

When designing a data governance policy, it is important to consider how the policy will be implemented and used. This requires thinking through the various roles and responsibilities various stakeholders have, and outlining them. Generally, there are four main stakeholders for data that is managed by a municipality:

- **City staff and leadership -** These groups should be informed about the policy and be held responsible for compliance.

- **Private sector -** The private sector should be informed about the policy, and be held responsible for compliance in procurement processes.

- **Public, and civil society -** The public and civic society should be informed about the policy, but can also be an active participant in its development. By treating data as a service, the public and civil society become clients for the city's open data.

- **University systems -** Academia uses data as a service to power research and innovation. Cities should consider how to build data sharing agreements with university partners that fast-track research while prioritising privacy and security.

Governing data governance

Data governance is a collaborative effort, and as such it will take a dedicated team to implement the procedures your policy puts in place. For a data governance policy to be successful, it's critical to have a mechanism to enforce, operationalise or otherwise implement it. Allocating resources to support implementation requires buy-in from city leaders, and any department leadership that will be involved in supporting the policy. Having a dedicated champion, or "tactical team" that continues to socialise the policy with stakeholders is key to achieving organisation-wide results. Here are some key components for governing data governance:

- **Develop a "guidelines" workspace:** If your policy is legally binding, is an executive order, or is enforceable, it may also reflect the most conservative approach to data governance. However in the future, your data governance policy may need to address topics in emerging technologies, such as blockchain or artificial intelligence. Therefore, it is handy to have a set of guidelines that are not enforceable policy, but allow you to provide preliminary "softer" provisions for topics in data governance that are not yet mature enough for inclusion in an enforceable directive. These guidelines can undergo regular review to determine their appropriateness for inclusion in an enforceable policy.

- **Establish an annual review committee:** A data governance policy is a living document, and should be revisited and revised especially with the rapid pace of innovation in technology and data science. The committee should determine if the policy is meeting its intended goals, is feasible to implement, and revise accordingly.

- **Establish a data governance taskforce:** Create a core team with members across relevant departments such as information technology, smart cities, procurement, legal, or the mayor and city manager's offices. The core team should be charged with ensuring implementation of the policy across city departments, and developing the tools and technologies to do so. The taskforce should report directly to city leadership on a regular cadence.

- **Establish a steering committee:** Steering committees help build the bridge between city staff implementing the policy, and the highest levels of city leadership. The data governance task force previously mentioned should report to the steering committee, which can be made up of executive level leadership, who can ensure buy-in across city department leadership.

- **Establish an advisory group:** To ensure transparency, you can create an advisory group of external experts from civil society and academia, who can advise on the policy's content, and support its ongoing development.

GOAL #2 Build public and internal data platforms that operationalize your data governance directive

City departments are notoriously siloed, and similarly the lack of data exchange between departments inhibits them from understanding the full picture of service demand and delivery. As a result most city departments tend to view their services as inherent to their department, rather than connected to a broader user experience across the municipality. Data platforms are one way that city departments can leverage data for collaboration, and reduce organisational and technological siloes. Building data platforms to operationalize data governance calls for additional reflection around the parameters of data sharing, including permissions, monetization, and the organisation's open data policies.

Cities globally have started developing open-data platforms and data directories that provide city departments with greater access to available data. For example, the City of Portland and Seoul are constructing their own internal data platforms to facilitate data sharing for city departments, including Portland Urban Data Lake and Smart City Seoul.

A data governance policy requires software, digital tools and platforms in order to make the shift from policy to action. One of the goals of data governance is to make data more searchable, accessible and safely shareable

within the organisation and with trusted partners. When data is classified as open, however, it should automatically be uploaded into an open data platform for public consumption, unless a data monetization strategy is in place. Open-data platforms should have integrated back-end databases that permit access by external applications, and prioritise back-end interoperability as a priority in their digital governance policies. As discussed, there are two types of digital platforms that can facilitate the operationalisation of a data governance policy.

- **Internal or "enterprise" data sharing platforms -** This type of platform is accessible only to authorised users internal to the organisation. It should allow users to classify datasets that they own, and include a searchable catalogue. One of the main purposes of an enterprise data sharing platform is that data transactions and classifications made under the policy can be easily audited.

- **Open data platforms -** An open data platform should have three main elements: 1) it identifies data sources, owners and acceptable use, 2) it should have a mechanism for data ingestion, classification, validation and **metadata,** and 3) it should facilitate accessibility and automatic downloads of data (typically through APIs). The Global Smart Cities Alliance provides several considerations and a model policy for how city governments can launch their own open data portals and programs[30].

GOAL #3 Build a program to train city departments on your data governance directive and implement a data governance policy

People power a data governance policy, and in many cases changing how data is managed in an organisation requires a cultural change. Integrating best practices in data governance into your organisation is not easy, and doing so requires dedicated capacity. However, without addressing implementation through training and culture change, the policy is not likely to be adopted and used. Therefore, it's very important that any group working to establish data governance in their city government think carefully about how the policy will be understood and acted upon by city staff.

The process of culture change should be as accessible as possible. City departments already struggle with capacity, and may not immediately be incentivised to adopt a new, comprehensive approach to data management. Champions of data governance need to clearly demonstrate the value for city departments, whether that be cost savings, increased access to data, more accurate performance evaluation, public transparency or enhanced collaborations with external partners. For buy-in to be achieved, and data governance to be sustained both operationally and culturally, city departments should be trained in values and procedures of data governance. What follows are recommendations for establishing culture change toward **data-informed government** in your organisation.

- **Establish a dedicated team to steward the program.** Ensure the team has access to city leadership and cross-cutting positions that can amplify the message.
- **Create a way to evaluate and report department progress towards data governance goals.** This can take the form of dashboards or regular reports to city leadership.
- **Assign dedicated staff or 'liaisons' in each department to ensure city department compliance.** Request that each city department dedicate a team member as a "data steward" who is responsible for the department's compliance with the policy.
- **Establish a platform for training** - Create a portal where resources are accessible to data stewards and city leadership. You can provide training materials, videos or other resources for self-directed learning.
- **Build an academy training program** - Train data stewards in cohorts, in a classroom style setting that can double as an opportunity to strengthen relationships and collaboration across departments.
- **Create a community of practice for trainees** - Shifting data governance culture may take years, and therefore its beneficial to create a space for data stewards and city staff to share ideas, troubleshoot, and collaborate on data-driven efforts.

BOX 3.2

City of San Antonio's Innovation Academy strategy

https://medium.com/what-works-cities-certification/innovation-problem-solving-for-the-people-in-san-antonio-4b66015357c8

In 2020 San Antonio launched the City's Innovation Academy, which is a joint project of the Office of Innovation, the City's HR department, and Alamo Community Colleges (ACC). The Academy trains creative problem-solvers across city departments who have leadership potential and a proposed innovation project toward which they want to apply new skills. ACC offers city staff intensive courses customised to meet the needs of the City in three specific areas: process redesign, human-centred design, and data analytics. The Innovation Academy's current cohort comprises senior leaders from across departments and members of the IT department. The idea is that mixing staff from different parts of government helps break down silos, and Academy graduates will pass on their knowledge to colleagues and the staff they manage.

GOAL #4 Identify opportunities to create new participatory processes involving data

Data governance helps make data more accessible to the public, and as a result new opportunities are unlocked to use open data for planning and participatory processes. Open data can be used to build community technology skills, host community workshops, and create new ways for communities to provide feedback about public data sets. People-centred smart cities should focus on building *with* community, rather than for the community. Doing so requires meeting communities where they are, in the spaces they choose, and integrating the use of data into pre-existing contexts.

Use open data to create skills training and workforce development opportunities

Data analysis requires skill, digital literacy and access to technology. When publishing open data, local governments should consider expanding access to that data by offering skills training for residents, and prioritising those typically in unserved or underserved communities. Training can provide residents with basic information about how to access and use an open data portal, or can go further to include basic data analysis skills. Such training and workshops can often have tremendous value to residents seeking to build new skills in order to be more competitive in the digital economy. For example, the Los Angeles Department of Neighbourhood Empowerment runs a Data Literacy Program to help neighbourhood groups make better use of the city's data. Freetown, Sierra Leone, hosts open data programs such as a data literacy boot camp that build capacity of local communities to generate and use open data through different tools and platforms.

Have conversations with residents about critical issues related to data in smart cities

Studies increasingly show a growing concern among the international public about data collection, privacy, and transparency. A recent study by Internet Society which polled consumers in Australia, Canada, Japan, France, the UK, and the US found that 75% of respondents distrusted how their data was managed and shared[31]. This poses a tremendous opportunity for local governments to explore ways of building trust and open dialog with residents about key issues in data, including bias in data collection and survey development, surveillance, and privacy. By being proactive about introducing opportunities to engage residents on these topics,

municipalities can avoid backlash that can occur when residents are not informed, consulted, or brought in as participants in smart city technology deployments[32]. Several cities have initiated these types of conversations with residents. For example, the City of Boston's New Urban Mechanics division "Digital Transparency in the Public Realm" project provides real-world information about data collection in public spaces, in order to start a dialog about transparency with residents[33]. Bangalore's Next Bengaluru program, uses technology coupled with a mobile waggon to engage residents on their perspectives while touring neighbourhoods.

Building engagement with communities using data

Data can help make lived experiences visible, and has tremendous power to expand municipalities' awareness of urban challenges faced by marginalised groups. Governments should actively seek ways to empower residents to tell their own stories using data, or otherwise work with marginalised groups to explore lived experiences that are not typically visualised or analysed. Doing so requires defining the community you want to work with, partnering with community-based organisations, meeting communities where they are, and centering the community's voice in data collection processes[34]. For example, the Detroit Digital Justice Coalition holds community workshops focused on identifying potential benefits and harms of data provided on the City of Detroit's open data platform, and has developed a set of recommendations for citywide adoption of open data[35]. Singapore's collaboration with Hello Lamp Post, allowed residents to exchange SMS-based dialog with objects in public space[36].

Invite citizen science and crowdsourcing opportunities

In citizen science, the public participates voluntarily in the scientific process, including collecting and analysing data, conducting scientific experiments, making new discoveries, developing technologies, and solving complex problems[37]. Crowdsourcing refers to distributed problem solving, where an organisation issues an open call for voluntary assistance from a large group of individuals online. Local governments strapped for capacity resources, can leverage citizen science and crowdsourcing to not only engage residents with open data, but also to collect new datasets, or solve problems in new ways by leveraging the experience and expertise of a diverse group of people. For example, Cape Citizen Scientist is a program that engages the public in a survey of plant pathogens in the Cape Floral Region in South Africa, and City Nature Challenge leverages citizens to catalogue and map their urban nature environment in Ahmedabad, India.

Citizen science, as a convergence of open science and open innovation, has proven to be an effective way to bridge the capacity gap for governments, while engaging residents as experts along the way. The US Federal government recently published a toolkit that provides guidance for how to launch a citizen science program. Making Sense, a consortium supported by the European Commission, has also published a toolkit for developing citizen participation in environmental monitoring and action, otherwise known as "citizen sensing".

04

ACTIVITY 7:

Safeguard public trust by protecting smart city assets

SDG 16, 16.6.
New Urban Agenda 157

Core Values

1 Approriate use of data

Value 1: Consensus about the appropriate use of data and smart city technology should be developed iteratively, and through the participation of many stakeholders.

2 Oversight on use of technology

Value 2: Residents should have clear oversight of the use of technology, particularly in public space, by local governments.

3 Implement regulations

Value 3: Local governments need to adopt comprehensive regulations, implement solid cybersecurity strategies and protocols, develop organisational risk-awareness, and leverage the appropriate tools to address the security issues generated by emerging smart city technologies.

Introduction

Trust is a key ingredient for any city that leverages data and technology to improve public services. As of 2019, only 45% of citizens in OECD countries believed they could trust their government[38]. In a digital world, building public trust requires transparency, meaningful public participation and meaningful consent in addition to **cybersecurity** measures that protect data and infrastructure.

Cybersecurity laws and policies have a direct impact on human rights, such as the right to privacy, freedom of expression, and the free flow of information[39]. City governments regulating such technology from a security standpoint should take care to educate residents on cybersecurity issues, be transparent about adopted cybersecurity policies or laws, and take a human-rights approach to cybersecurity strategy. They must also acknowledge that cybersecurity risks are not experienced evenly by everyone, and that minorities and marginalised groups may experience disproportionate risk when using digital public services.

The reliance on computer systems by local governments means that critical infrastructure such as transportation systems and energy grids are more exposed to cyberattacks that can result in large-scale service disruptions. Smart city technologies that transmit data from devices and infrastructure across the internet also introduce new security vulnerabilities for cities, because if left unsecured, these systems can potentially be intercepted and exploited. Likewise, unprotected data used to deliver digital services can be accessed by attackers to obtain sensitive or personally identifiable information, further exposing local governments to the risk of fraud, ransom, and theft. Even further, unproven and untested smart city technologies can pose risks to human rights as they have the potential to be misused. These risks increase when governments outsource services and software development to third party developers. A report endorsed by the Africa CyberSecurity Conference estimated that the continent lost about $3.7 billion dollars to cybercrime in 2017[40]. The threat of cybersecurity attacks has become so prevalent, that municipal bond investors are increasingly accounting for a city's cyber preparedness when issuing bond ratings[41].

As cyberthreats for cities continue to grow, local governments are under growing pressure to take action, and balance cybersecurity policy with human rights. Fortunately, city governments can take significant steps towards cybersecurity readiness without spending a lot of money on digital infrastructure. Because cybersecurity is not just an IT issue, a successful strategy must be part of an integrated approach that occurs at all levels of the organisation. This type of approach combines people, processes and technology through educational, legal, political, and technical means. A cybersecurity strategy will look different for different cities, but all approaches must start with a baseline understanding of the vulnerabilities and threat landscape pertaining to your unique context.

Successfully preparing your municipality for cybersecurity threats requires support and awareness across all levels of government, including appointed staff and elected officials. Local officials must understand the responsibility they have towards securing sensitive data and information within their departments, and influencing behaviour among their staff. By adopting comprehensive regulations, implementing solid cybersecurity policies and protocols, developing organisational risk-awareness, and leveraging the appropriate tools, cities stand a greater chance of addressing the security issues generated by emerging smart city technologies.

To get started on building a baseline for cybersecurity readiness, we recommend three main goals:

- Identify any existing cybersecurity policies at the state, regional, or national level that pertain to your municipality
- Build a people-centred cybersecurity policy that is responsive to the unique needs of your community and respects human rights
- Identify areas of security risk within your municipality and take steps to manage those risks

BOX 4.1

Hiperderecho: Facilitating public awareness of cybersecurity in Peru

https://privacyinternational.org/long-read/3278/privacy-security-op-ed-peru
https://hiperderecho.org

Technology is redefining the way we exercise basic human rights such as freedom of expression, privacy, access to culture, or public information. These rights can come under threat by public policies that do not understand technology and its potential. Hiperderecho is a Peruvian non-profit civil association dedicated to research, facilitate public understanding, and promote respect for rights and freedoms in digital environments. Their involvement is divided between advocacy actions, such as public policy analysis, legal reform proposals and activism; and educational and training activities on digital rights for Peruvian students, activists and professionals. Example documents include guides for a Good Electronic Government, a Biometric Identity, Election Data and tutorials on how to reclaim our privacy and data.

According to the organisation, privacy is an excellent security policy. Organisers emphasise that governments need to establish clear rules and limits to their access to communications, and should set forward strict criteria for data processing activities. Hiperderecho's philosophy is that security should not come at the expense of privacy, but the opposite: privacy is security, and if we lose the first we cannot have the second.

GOAL #1 Identify existing cybersecurity policies at the state, regional, or national level that pertain to your municipality

There's no need to reinvent the wheel, and in many cases national governments already have cybersecurity policies, laws, or recommendations in place that impact local government. For example the United States Federal Government publishes cybersecurity standards that local governments can adapt to their own context[42], while Brazilian Instituto Igarapé publishes the Brazilian Cybersecurity Strategy[43] aimed at a national multi stakeholder approach. The International Telecommunication Union (ITU) maintains an index of national cybersecurity policies across the globe, and identifies which countries have national cybersecurity strategies, and cybersecurity incident response teams. The table below lists a handful of national security policies available by region to guide your search.

Table 1: National Cyber Security Policies by Region

Africa	Nigeria	South Africa	Kenya	Burkina Faso
Americas	USA	Mexico	Canada	Brazil
Arab States	UAE	Morocco	Saudi Arabia	Egypt
Asia Pacific	Singapore	China	Malaysia	Thailand
CIS	Russian Federation	Kazakhstan	Azerbaijan	Belarus
Europe	UK	France	Denmark	Spain

GOAL #2 Build a people-centred cybersecurity policy that is responsive to the unique needs of your community and respects human rights

Cybersecurity policies should identify procedures, resources, roles, and responsibilities within your organisation that reduce threats to the availability, confidentiality, and integrity of information and its underlying infrastructure, so as to preserve the security of networks and ultimately people both online and offline. A cybersecurity strategy covers the security of both information and physical infrastructure, including but not limited to physical and cloud infrastructure, devices, networks, data, applications, and users. A human rights based approach to cybersecurity makes provisions to address the security, privacy, and autonomy of residents and vulnerable groups.

What should be in a cybersecurity policy?

A robust cybersecurity policy should focus on more than just the technical aspects of security. It should also include approaches grounded in education, and training approaches that aim to shift an organisation's culture towards prioritising security of digital assets. Cybersecurity policies can be a single document, or a compilation of documents that address key areas of risk assessment, asset protection, response, and recovery. Below is a list of some of the items that should be included in a municipal cybersecurity strategy, adapted from the G20 Cyber Accountability Model.

- **Risk assessment** - *Identifies key vulnerabilities, and outlines a routine process for evaluating cybersecurity risks. The risk assessment should identify the categories of risk that apply across people, processes, systems, and vendors.*
- **Roles & responsibilities** - *Defines who is responsible for each aspect of cybersecurity readiness, with clear roles outlined for senior leadership.*
- **Security of information assets** - *Minimum standards (including for procurement of new ICT deployments) for the security of the city's information assets, for all IT/OT infrastructure. This can also include a password management policy, and introduce multi-factor identification measures.*
- **Security of physical devices** - *Policies that address how municipal devices such as laptops, desktops and cell phones will be secured and outline steps to enforce the policy.*
- **Prevention policies and processes** - *Proactive policies and processes that reduce the risk of a cybersecurity threat. This can include security training for employees, routine software updates, backing up critical data, user control access, and encryption policies.*
- **Response policies and processes -** *Measures, procedures and steps that will be taken in the event of an incident.*
- **IT risk management and security training** - *Tools, resources and trainings either required or offered to employees to increase the level of cybersecurity awareness and best practices.*
- **Cybersecurity standards for third parties** - *Security standards and procurement requirements for third parties that build software, digital tools, programs, services or infrastructure.*
- **Public engagement on cybersecurity risks** - *Educational campaigns that aim to increase awareness and preparedness for cybersecurity threats among the general public.*

Additionally, the National Institute of Standards and Technology (NIST) provides a Cybersecurity Framework Policy Template Guide that includes policy templates for five stages of cybersecurity readiness: Identify, Protect, Detect, Respond and Recover[44].

A human rights based approach to cybersecurity

A human rights based approach to cybersecurity prioritises the rights of citizens to privacy and freedom of speech, among others. It also takes steps to address how marginalised groups are disproportionately at risk when using the internet and digital services, by creating policies and standards in place for technology procurements and deployments that are privacy-preserving. The Association for Progressive Communications (APC 2020) defines a human rights-based approach to cybersecurity as one that "ensures that there is trust and security in networks and devices that reinforce, rather than threaten, human security." Broadly there are three key areas that can help bolster the inclusion of human rights in cybersecurity policy:

1. Frame cybersecurity challenges around individuals, recognizing that their interactions with digital public services generate sensitive personal information that should be protected.

2. Ensure transparency of public-private partnerships which arise as government institutions outsource their administration and security needs to the private sector, and that such partnerships are subject to rigorous accountability mechanisms

3. Build cybersecurity laws and policies that are designed to respect and protect human rights, including the freedom of speech, privacy and the free flow of information.

GOAL #3 Identify areas of security risk within your organisation and take steps to manage these risks

Security risks will look different for each municipality depending on your local and regional context. However, there are several common cybersecurity threats associated with smart cities and local governments that all cities can prepare for. Below are four areas of current growth that should be accounted for in today's cybersecurity strategies.

- **Internet of Things (IoT)** - IoT deployments pose a cybersecurity risk because they transmit data, and often sensitive data across internet networks. Adopting security requirements for IoT deployments and procurements from third parties can help ensure that IoT deployments are secure. NIST provides cybersecurity guidance for IoT technology.

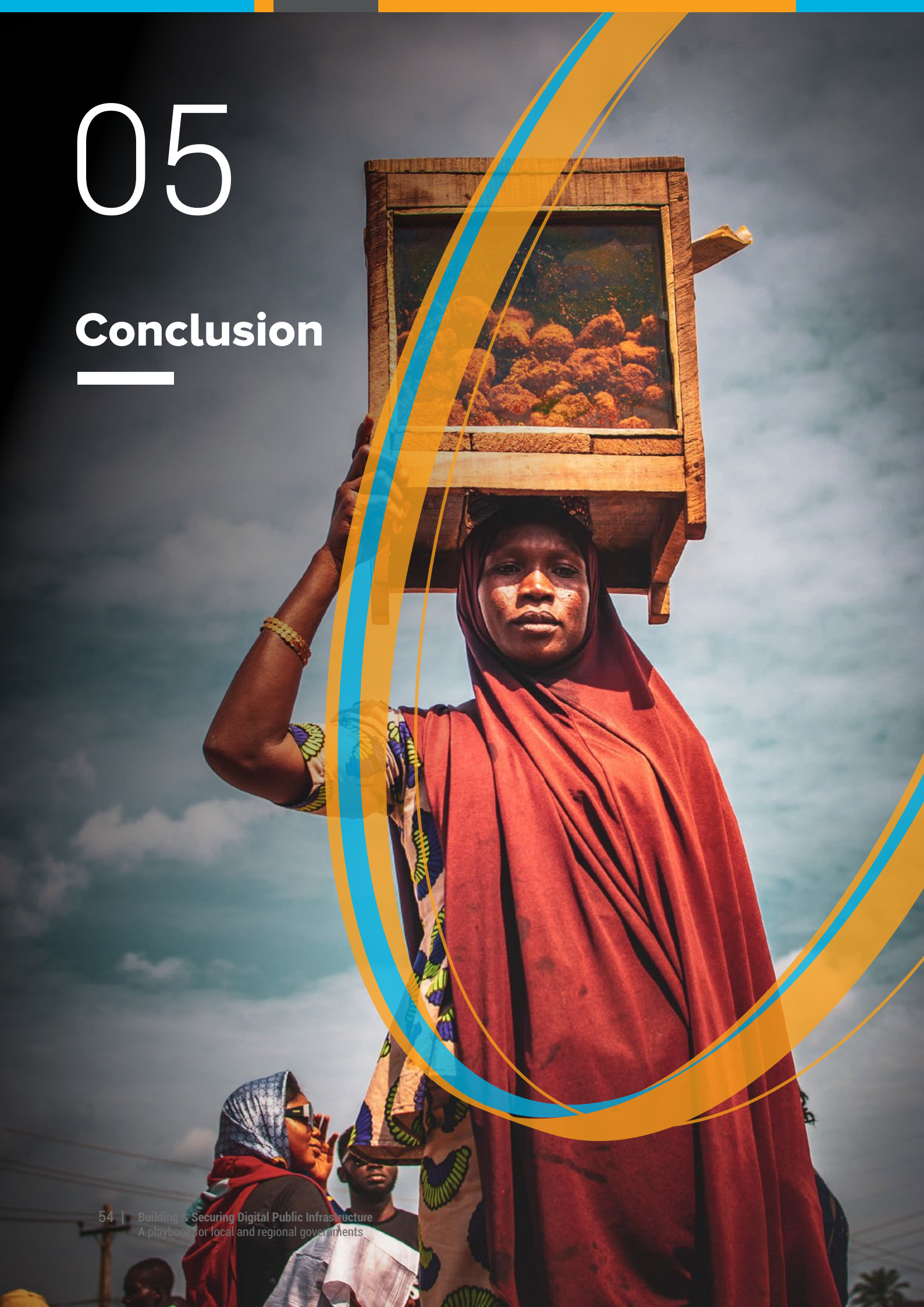
- **Remote Work -** There are several risks associated with remote work, including when employees use personal devices for work, access sensitive data from unsecured networks, or use unencrypted file sharing. Creating a remote work cybersecurity policy, and enforcing security measures like multi-factor identification, **virtual private networks (VPNs)**, and firewalls can help reduce the risk incurred by remote work.

- **Cloud Computing -** Cloud computing refers to on-demand availability of computer system resources, especially data storage and computing power. Common risks for cloud computing include risks to malware exposure, ensuring that cloud companies comply with security laws and policies, and having limited visibility of network operations. To reduce these risks, take steps to confirm that any cloud computing companies adopt strict security policies.

- **Third party software integrations -** Third party software integrations occur when any program or application that is not written exclusively by employees is connected to existing internal systems. There are several risks posed with this and strategies to address them. McKinsey & Company provides a useful guide to enterprise cybersecurity that addresses these risks and approaches.

05

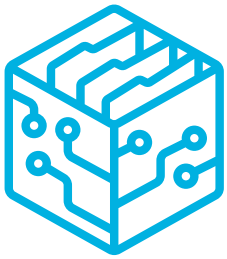
Conclusion



People-centred smart cities need accessible, secure, and fair digital public infrastructure that powers digital services, and ensures everyone has equal opportunity to fully participate in civic life. The urgency for the development of digital infrastructure is compounded by the demand that has increased following the CoVID-19 pandemic for trustworthy and reliable digital services. However, many local governments and some national governments feel they do not currently have the digital literacy, capacity or expertise needed to build the infrastructure required to power smart public services. As a result, there are significant risks posed by an overreliance on third parties to build and maintain digital infrastructure. Municipalities that want to expand their capacity for building digital infrastructure through public private partnerships, should take great care to ensure their ability to maintain the interoperability, accessibility, and control over digital assets and the data they generate. Doing so is vital to the ability of local governments to guarantee public interest, and safeguard human rights.

This playbook highlighted a set of activities local and national governments can do in order to achieve specific goals enabling the development of digital public services, and the security of the data and digital infrastructure that powers them.

Specifically, cities that want to build people-centred smart cities should strive to:



1

Improve the convenience and accessibility of services by digitising them

2

Create a data governance framework that sets standards and responsibilities for effectiveness, accountability and inclusivity,

3

Safeguard public trust by protecting smart city assets

We believe these three activities and their associated goals can help local governments build people-centred digital services that prioritise human rights and more effectively address the needs of all those who live, work and play in cities. The challenge for cities will be to balance the promise of emerging technology with privacy, accessibility, transparency and security. These core values are critical to building people-centred smart cities that **realises sustainability, inclusivity, prosperity and human rights for the benefit of all.**

Endnotes

1 https://unhabitat.org/un-system-wide-strategy-on-sustainable-urban-development https://unsceb.org/united-nations-system-wide-strategy-sustainable-urban-development

2 Measuring Digital Development: Facts and Figures 2020, International Telecommunication Union Development Sector (ITU).

3 UN Human Rights & Social Inclusion Unit

4 The UN Hub for Human Rights and Digital Technology.

5 The Secretary-General's Independent Expert Advisory Group (IEAG) on a Data Revolution for Sustainable Development report 'A World that Counts'.

6 "Cybersecurity and Human Rights," Carolina Rossini and Natalie Green, Public Knowledge 2015.

7 https://www.scmp.com/news/china/article/1114741/critics-fear-npcs-new-rules-digital-information-will-stifle-internet

8 https://www.thelocal.se/20131013/50760/

9 https://www.brookings.edu/techstream/designing-digital-services-for-equitable-access/

10 https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf

11 New America's Digital Impact and Governance Initiative

12 https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id

13 "Catalog of Technical Standards for Digital Identification Systems" World Bank Group, 2018.

14 "What happens when a billion identities are digitized?" Yale Insights, 2020.

15 "Privacy by Design - the 7 foundational principles," International Association of Privacy Professionals (IAPP), 2022.

16 "2021 Annual Report," Identification for Development, 2021.

17 Better than Cash Alliance: https://www.betterthancash.org/

18 Payment aspects of financial inclusion (English). Washington, D.C. : World Bank Group. http://documents.worldbank.org/curated/en/806481470154477031/Payment-aspects-of-financial-inclusion

19 "Building Inclusive Digital Payments Ecosystems: Guidance Note for Governments," https://btca-production-site.s3.amazonaws.com/documents/293/english_attachments/GPFI_Guidance_Note_Building_Inclusive_Dig_Payments_Ecosystems_final_0.pdf?1499784653

20 "PIX: The new instant payment system from Central Bank of Brazil," https://business.ebanx.com/en/resources/payments-explained/pix-instant-payment-system.

21 Igniting SDG Progress through Financial Digital Inclusion," Better than Cash Alliance, 2022.

22 "Success Factors in Tax Digitalisation," Better than Cash Alliance, 2020.

23 "Tax digitalization: building a trusted ecosystem through a common vision," Better than Cash Alliance Learning Series, 2022.

24 "7 hunger deaths related to Aadhaar," The Times of India, 2018.

25 https://www.npr.org/sections/goatsandsoda/2017/01/11/503159694/blockchain-could-be-a-force-for-good-but-first-you-have-to-understand-it

26 "Registering property: the paths of digitization," The World Bank, 2015.

27 "A roadmap for digitising source-to-pay," McKinsey & Company, 2017.

28 "Productivity in Public Procurement," pg. 97 OECD, 2019.

29 Beduschi, Ana. "Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations" Cambridge University Press, 2021.

30 "Open Data Model Policy", G20 Global Smart Cities Alliance, 2020.

31 "The Trust Opportunity: Exploring consumers' attitudes toward the internet of things," Internet & Society, 2019.

32 "San Diego Mayor orders Smart Streetlights Turned Off," Government Technology, 2020.

33 "Digital Transparency in the Public Realm," Office of New Urban Mechanics, 2021.

34 Angarita, Jennifer. "Amplifying Civic Innovation: Community Engagement Strategies for open data collaborations," Ash Center & City of Cambridge, 2016.

35 "Data Justice: Guidelines for Equitable Open Data," Detroit Digital Justice coalition, 2017.

36 "Singapore," Hello Lamp Post, 2015.

37 "About Citizen Science," Citizenscience.gov, 2016.

38 Trust in Government, OECD 2019.

39 "Cybersecurity and Human Rights," Carolina Rossini and Natalie Green, Public Knowledge 2015.

40 https://www.africacybersecurityconference.com/

41 https://www.govpilot.com/blog/municipal-bond-ratings-yet-another-reason-to-enhance-cybersecurity

42 https://www.nist.gov/cybersecurity

43 https://ciberseguranca.igarape.org.br/en/

44 "NIST Cybersecurity Framework Policy Template Guide", National Institute of Standards & Technology, 2022.

Terms & Definitions

Application programming interfaces (APIs)
A software intermediary that allows two computer applications to exchange data and information.

Assistive technologies
Products, equipment, and systems that enhance learning, working, and daily living for persons with disabilities.

Automated decision-making
Automated decision-making is the process of making a decision by automated means without any human involvement.

Big Data
Big Data is a collection of data with specific and simultaneous characteristics: huge in volume, high in velocity, diverse in variety in type, exhaustive in scope, fine-grained in resolution, relational in nature and flexible.

Blockchain
A blockchain is a digitally distributed, decentralised, public ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format.

Cybersecurity
The preservation – through policy, law, technology, best practices, cooperation, and education of the availability, confidentiality, and integrity of information and its underlying infrastructure, so as to preserve the security of networks and ultimately people both online and offline.

Data portability
Data portability is the ability to move data among different applications, programs, computing environments or cloud services.

Data governance
Refers to the collection of policies, processes, and standards that ensure the quality, integrity, security, availability, usability, and accessibility of a city's data assets while respecting residents' rights to privacy.

Data-informed government
The ability of a government to develop policies, programs, and decision-making informed by data in addition to other forms of expertise and contextual information.

Data sovereignty
Data sovereignty is the idea that data is subject to the laws and governance structures that govern where it is collected. The concept of data sovereignty is closely linked with data security, cloud computing, network sovereignty and technological sovereignty.

Data Stewards
Individuals designated to manage data governance activities within their department or organisation.

Digital identification
A digital identity is a collection of features and characteristics associated with a uniquely identifiable individual — stored and authenticated in the digital sphere — and used for transactions, interactions, and representations online.

Digital twin
A virtual representation that serves as the real-time digital counterpart of a physical object or process.

Digitalising tax administration
This refers to the use of digital and data-driven approaches to optimise the functions and operations of revenue authorities. These include taxpayer registration, filing, compliance and audit, payment, and disputes, as well as broader taxpayer services and user experience.

Digital transformation
The process of using digital technologies to modify existing systems.

Digitisation
Digitisation refers to the process of changing from analog to digital formats, such as transforming paper currency into an electronic or digital store of value, increasing accessibility, and usability.

Digitalisation
Digitalization refers to the use of digital technologies to change an operating model and transform operational processes, providing additional revenue and value-producing opportunities

Digital public infrastructure
Digital public infrastructure refers to the tools and systems required to make digital life function in cities. Digital public infrastructure lets us experience public services, and engage in civic life through the use of the internet and online transactions.

Digital government services
Digital government services are defined as service delivery within government, as well as between government and the public, using information and communication technologies.

Digital service standards
A set of best-practice principles for designing and delivering government services.

Internet of Things (IoT) technologies
A global infrastructure for the information society enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving, interoperable information and communication technologies (Recommendation ITU-T Y.2060)

Interoperability
Refers to the ability of multiple technology systems to exchange information and to use the information that has been exchanged.

Key Performance Indicators (KPIs)
A quantifiable measure of performance over time for a specific objective.

Metadata
Metadata is data that describes other data, providing a structured reference that helps to sort and identify attributes of the information it describes.

People-centred smart cities
People-centred smart cities leverage data, technology and services for common good, delivering the inclusive and sustainable cities that are needed in the 21st century.

Personally identifying information (PII)
Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Source-to-pay
Source-to-pay is the end-to-end value stream that encompasses all the activities required for an organisation to obtain and pay for goods and services from other entities.

User centred or "UX" design
An iterative design process in which designers focus on the users and their needs in each phase of the design process.

Vendor lock-in
A situation in which a customer using a product or service cannot easily transition to a competitor's product or service.

Virtual private networks (VPNs)
An encrypted connection over the Internet from a device to a network.

Activity 5 Policy Resource Kit:

Improving the convenience and accessibility of services by digitising them.

Activity 5 addresses how to undertake digital transformation within your organisation starting with three key steps. The first step is to establish a set of community-driven digital standards that provide uniform commitments across all digital services provided by your organisation covering privacy, equity, security, and interoperability, among other things. Digital service standards create a guideline for any department seeking to improve or deliver a digital public service. Once digital standards are in place, organisations can proceed to develop the "civic technology stack," which refers to key areas of digital transformation. For local governments, these key areas include digital identity, digital payments and data exchange.

Finally, it is important to build the capacity necessary for your government's digital transformation. Any digital service that is built must be maintained and supported by a management structure that ensures the longevity of the service. How you 'govern' digital transformation will look different for different communities, but all models should centre on transparency and collaboration.

Below are resources and examples to guide your digital transformation efforts.

Digital service standards

Examples of digital service standards in practice.

Digital Service Standard - Open source, global

Australia - https://www.dta.gov.au/help-and-advice/about-digital-service-standard

UK - https://www.gov.uk/service-manual/service-standard

Wales - https://digitalpublicservices.gov.wales/toolbox/digital-service-standards/

Ontario - https://www.ontario.ca/page/digital-service-standard

Singapore - https://www.tech.gov.sg/digital-service-standards/

Taiwan - https://www.ndc.gov.tw/en/Content_List.aspx?n=E35FD251AA134CA4

Barcelona - https://www.barcelona.cat/digitalstandards/en/digital-services/0.1/

Brazilian Digital Services - https://www.gov.br/governodigital/pt-br/transformacao-digital/ferramentas/modelo-de-qualidade-dos-servicos-digitais/padroes-de-qualidade-para-servicos-publicos-digitais

The Civic Stack

What to consider when building out the three key areas of digital transformation.

Digital Transformation Toolkit Navigator, Observatory of Public Sector Innovation

A Data Driven Public Sector: Enabling the strategic use of data for productive, inclusive, and trustworthy governance, OECD.

Digital Defence Playbook, Our Data Bodies.

Catalogue of Technical Standards, World Bank

Tax Digitalisation, The Better than Cash Alliance

Activity 6 Policy Resource Kit:

Create a data governance framework that sets standards and responsibilities for effectiveness, accountability and inclusivity.

Data governance is critical to smart city development. Data governance refers to a collection of policies, processes, and standards that ensure the quality, integrity, security, availability, usability, and accessibility of a city's data assets while respecting residents' rights to privacy. Municipal governments can develop data governance by creating enforceable policies, and then leveraging those policies to build capacity and funding to support data governance programming.

At its core, a data governance policy provides the core values that guide your organisation's understanding of the role data plays in your government and community. It will also establish procedures for how to manage and secure data from the point of collection, through its use and disposal. This requires the creation of digital infrastructure such as data sharing platforms to operationalize such procedures. Finally, a data governance policy creates roles and responsibilities for stakeholders involved in each step of the process. Without these roles and responsibilities clearly defined, a data governance strategy cannot succeed. This toolkit provides examples and frameworks for the development and operationalization of data governance policies in local government.

Data governance frameworks

Guidance for developing data governance.

What Works Cities Certification Program, Bloomberg Philanthropies

DataSmart Cities, Empowering Cities through Data, India National Government

A Commons Approach to Smart City Data Governance, New America

Open Data Policy Toolkit, G20 Global Smart Cities Alliance

Data governance policies in action

Examples of existing data governance policies in practice.

- Barcelona has published "Ethical Digital Standards Toolkit" that includes a Data Governance and Policies Section.
- San Francisco published a Data Quality Guidebook for both users of their Open Data Platform, and City Departments. They also published a Data Coordinator's Guidebook for City Departments with a designated Data Coordinator.
- The city of New York created Local Law 11 in 2012, legislating their data governance policy for open data and open standards. NYC has also created a privacy policy governing the use of IoT.
- City of Tulsa has a Data Policy that references several sub-policies including AI. The data manual includes more detail.
- Portland City Council passed Data Privacy & Information Protection Principles and established an internal Privacy Work Group to determine implementation. The principles are part of the Smart City PDX Framework which addresses technology disparities and information management. A City Council resolution establishes the framework, and makes commitments to implement.

Activity 7 Policy Resource Kit:

Safeguard public trust by protecting smart city assets.

This activity addresses how municipalities can secure smart city assets. To get started on building a baseline for cybersecurity readiness, we recommend three main goals. First, local governments should work to identify any existing cybersecurity policies at the state, regional, or national level that they are subject to. Secondly, local governments should consider building a people-centred cybersecurity policy that is responsive to the unique needs of your community and respects human rights. Several examples exist of such policies. Finally, local governments can identify key areas of security risk within their organisation and by doing so, take steps to manage those risks. This toolkit provides a handful of useful models for building, developing and executing cyber security policies and strategies.

Cybersecurity models

Cybersecurity Challenges and the Way Forward for Developing Countries, Institute of Electrical and Electronics Engineers (IEEE).

Playbook: Government as a Platform, ASH Center for Democratic Governance & Innovation, Harvard Kennedy School.

E-Estonia Toolkit, Estonian National Government

Cyber Accountability Model, G20 Smart Cities Alliance

"NIST Cybersecurity Framework Policy Template Guide", National Institute of Standards & Technology


NIKE

www.unhabitat.org

UN HABITAT
FOR A BETTER URBAN FUTURE

UNITED NATIONS HUMAN SETTLEMENTS PROGRAMME
P.O. Box 30030, Nairobi 00100, Kenya
T: +254-20-76263120
E: infohabitat@unhabitat.org

UN-HABITAT
@un-habitat

IMPLEMENTING THE NEW URBAN AGENDA

11 SUSTAINABLE CITIES AND COMMUNITIES