FOSTERING CIVIC TRUST

A POLICY GUIDE FOR MUNICIPAL LEADERS

THE NATIONAL SCIENCE FOUNDATION IS FUNDING THIS WORK IN PART UNDER COOPERATIVE AGREEMENT 2044448

TABLE OF CONTENTS

ACKNOWLEDGEMENTS 5

INTRODUCTION 7

SECTION 1. DATA GOVERNANCE 11

Overview 11

Key Definitions 12

Why do we care? 12

1.1. Establishing a Data Strategy and a Model Data Policy for Good Data Governance 13

1.1.1 What is a data strategy? 13

1.1.2 Why should cities and communities have a data strategy? 13

1.1.3 What are some good examples of a data strategy? 13

1.1.4 What is a data policy? How is it different from data strategy? 14

1.1.5 Why a data policy is needed? 14

1.2. Key Aspects of Data Governance 15

1.2.1 How can cities and communities identify what data are being collected? 15

1.2.2 Why should cities and commuinities create data inventories? 15

1.2.3 What roles and responsibilities should be assigned? 16

1.2.4 How can cities and communities classify data? 17

1.2.5 How can cities and communities define data access? 17

1.2.6 How can cities and communities ensure the quality of data? 18

1.2.7 What is data retention and destruction? 18

1.2.8 How can cities and communities preserve data in case of an equipment failure, natural disaster, or cyberattack? 19

1.2.9 How can cities and communities use data efficiently? 20

1.2.10 How can cities and communities ensure data oversight? 21

1.3. Key Considerations for Data Sharing 21

1.3.1 What is data sharing and integration? 21

1.3.2 What are the risks and benefits of data sharing? 22

1.3.3 What roles do data professionals play in data sharing? 22

1.3.4 What are data sharing agreements? 23

1.3.5 What are the different types of data sharing agreements? 24

1.3.6 How should cities and communities respond to data requests? 25

1.3.7 How can cities and communities approach data de-identification/anonymization for responding to data sharing requests?. 25
1.3.8 How can we prepare for a successful data request? ... 26
1.4. Understanding Open Data ... 27
1.4.1 What is open data and what are its guiding principles? ... 27
1.4.2 How can cities and communities start to open up data? ... 27
1.4.3 What is an Open Data policy and how can cities and connected communities draft an Open Data Policy? ... 29
1.5. Data Governance Resource Repository for Cities and Communities ... 30
SECTION 2. CYBERSECURITY ... 33
Overview ... 34
Key Definitions ... 35
Why do we care? ... 35
2.1. Understanding Cybersecurity Governance ... 36
2.1.1 What is cybersecurity governance? ... 36
2.1.2 Who should be involved in cybersecurity governance? ... 36
2.1.3 What is an information security policy and why is it important? ... 37
2.1.4 How can cities and connected communities draft a security policy? ... 37
2.1.5 What are some frameworks and standards for managing cybersecurity risk? ... 38
2.2. Understanding Cyberattacks ... 39
2.2.1 What is a cyberattack? ... 39
2.2.2 Who are cyber attackers? ... 40
2.2.3 What are the different types of cyberattacks that cities and communities should know about? ... 40
2.2.4 How do cyberattacks work? ... 41
2.2.5 What is the cyber boom model? How does it help cities and communities approach cybersecurity? ... 42
2.3. Best Practices in Cybersecurity ... 43
2.3.1 What best practices cities and communities can adopt to prevent and protect from cybersecurity incidents? ... 43
2.3.2 What are the best practices during a cyberattack (left of boom)? ... 46
2.3.3 What are the best practices after a cyberattack (right of boom)? ... 47
2.4. Cybersecurity Resource Repository for Cities and Communities ... 48
SECTION 3. PRIVACY ... 51
Overview ... 52
Key Definitions ... 53
Why do we care? ... 53
3.1. Establishing Privacy Principles and Policies ... 54
3.1.1 What are privacy principles? ... 54

3.1.2 Why should cities and communities adopt privacy principles? 54
3.1.3 What are some of the prominent privacy principles? 54
3.1.4 What are the key considerations and common themes that are primarily addressed in privacy principles? 55
3.1.5 Are there any good examples of cities or communities that have adopted their own privacy principles? 56
3.1.6 How are privacy principles different from privacy policies? 57
3.1.7 What are the dos and don'ts of creating a privacy policy? 57
3.2. Creating Accountability for Privacy 59
3.2.1 What is the role of privacy professionals in creating accountability internally? 59
3.2.2 What are the key considerations for creating internal accountability? 59
3.2.3 What are the key considerations for creating external accountability? 60
3.3. Evaluating Privacy Risk 61
3.3.1 What can cities and communities do to evaluate technology solutions offered by vendors? 61
3.3.2 How can cities and communities evaluate and monitor privacy risks? 62
3.3.3 Several cities and communities have limited resources and expertise to independently evaluate tech capabilities. How can cities and connected communities overcome this challenge? 64
3.4. Privacy Resource Repository for Cities and Communities 65
SECTION 4. COMMUNITY ENGAGEMENT 68
Overview 69
Key Definitions 70
Why do we care? 70
4.1. Understanding Community Engagement 71
4.1.1 What are the different levels of community engagement? How is the degree of public participation defined? 71
4.1.2 How can cities and communities' benefit from public engagement? 72
4.1.3 What are the principles of community engagement? 72
4.1.4 How can cities and communities scale trust through community engagement? 73
4.1.5 What approach should cities and communities take to community engagement? 73
4.2. Planning and Operationalizing Community Engagement 74
4.2.1 How can we build organizational capacity for Community Engagement? 74
4.2.2 How can we decide what degree of participation/engagement is required? 74
4.2.3 How can cities and communities draft their community engagement strategy/plan? 75
4.3. Ensuring Meaningful Community Engagement 76
4.3.1 How can cities and communities engage the right stakeholders for the community engagement efforts? 76
4.3.2 What different types of people should cities and communities engage and what can be done to encourage wide participation? 76

4.3.3 How should cities and communities select tools for inclusive community engagement? 78
4.3.4 How can online engagement facilitate broader and inclusive community engagement? 78
4.3.5 What are the best practices for ensuring an inclusive community engagement? 78
4.4. Community Engagement Resource Repository for Cities and Communities 80
SECTION 5. EQUITY 83
Overview 84
Key Definitions 85
Why do we care? 85
5.1. Understanding Equity 86
5.1.1 How should cities and communities think about equity and how is it different from equality and justice? 86
5.1.2 What are some of the key concepts that cities and connected communities should know to better understand equity? 87
5.1.3 What are the benefits of investing in equity-focused initiatives? 88
5.1.4 How can cities and communities get started with equity? 88
5.2. Operationalizing Equity 90
5.2.1 How can cities and communities embed equity in their operations? 90
5.2.2 How can cities and communities align data and technology programs with equity goals? 91
5.2.3 What are the best practices for creating equitable cities and communities? 92
5.3. Equity Resource Repository for Cities and Communities 94

ACKNOWLEDGEMENTS

US Ignite initiated the development of this guide for its network of smart and connected communities. These are more than three dozen communities addressing modern-day challenges through innovation, advanced networking technologies, and data-driven strategies. This guide solidifies our commitment to support these communities by sharing tools and best practices for building smart community strategies, services, applications, and sustainability plans that further social and economic opportunity.

The guide has benefited immensely from the insights of experts we interviewed and reviewers who gave their valuable feedback during the different phases of the review process. We would like to extend our sincere gratitude to the following experts and reviewers for their time and efforts to shape the guide.

EXPERTS:

	INTERVIEWEE	POSITION AND ORGANIZATION
Privacy	Kelsey Finch	Senior Counsel, Future for Privacy Forum
	Caitlin Fennessy	Research Director, IAPP, International Association of Privacy Professionals
Data Governance	Tim Moreland	Director of Performance Management and Open Data, City of Chattanooga, TN
	Kevin Comstock	Smart City Director, Transportation Department, City of Chattanooga, TN
	Dave Fletcher	Chief Technology Officer, State of Utah
	Barney Krucoff	Chief Data Officer, District of Columbia
Cybersecurity	Christos Papadopoulos	Professor and Sparks Family Chair of Excellence in Global Research Leadership, The University of Memphis
	David Balenson	Senior Computer Scientist, SRI International
Community Engagement	Charlie Catlett	Director, Array of Things, Joint Venture of Argonne National Laboratory and the University of Chicago
Equity	Joshua Edmonds	Director of Digital Inclusion, City of Detroit, MI
	Kiran Jain	COO, Resilient By Design
	Kellee Coleman	Business Process Consultant, Equity Office, City of Austin, TX
	Brandon Kroos	Business Process Consultant, Equity Office, City of Austin, TX

REVIEWERS:

	REVIEWER	POSITION AND ORGANIZATION
Privacy	Jamie Lees	Chief Data Officer, County of Arlington, VA
Data Governance	Drew Mingle	State Data Coordinator, State of Utah - Dept of Technology Services
Cybersecurity	Michael Dunaway	Executive Director, Digital Futures Resilience & Recovery Programs Office of Research, University of Cincinnati
Community Engagement	Deb Socia	President/CEO, The Enterprise Center
Equity	Joshua Edmonds	Director of Digital Inclusion, City of Detroit, MI
	Kellee Coleman	Business Process Consultant, Equity Office, City of Austin, TX
All	Holly Hartell	Assistant CIO, County of Arlington, VA
	Emily Yates	Smart City Director, City of Philadelphia, PA
	Hector Cardenas	Professor, Goldman School of Public Policy & CEO of Ergo Group

US IGNITE EDITORS

Glenn Ricart, Chief Technology Officer
Lee Davenport, Director of Community Development
Arnold Liyai, Program Manager
B'Asia Settles, Program Manager
Lizzette Arias, Communications Manager

AUTHOR

Jigyasa Sharma, Master of Public Policy '21

The author conducted this study as part of the Master of Public Policy (MPP) program at the Goldman School of Public Policy, University of California, Berkeley with support from US Ignite and the National Science Foundation.

INTRODUCTION

About one-third of smart city projects fail, and around 80 percent of prototypes fail to scale and reach their desired scope.[1] Smart city investment failures undercut civic trust and can have far-reaching economic and social consequences. We see too many smart community projects face severe public backlash when adoption of smart city applications conflicts with resident privacy and security. More often than not, municipal leaders fail to take into account the policy considerations that go into decision-making or allocate sufficient time to use community feedback to improve the projects. The guidebooks and policies that exist are excellent, but often don't reach their intended audience or motivate them correctly with accessible language. Smart and connected communities are a people problem as it goes beyond its technical considerations of privacy and cybersecurity. Whether you are leading a smart community now, or can't figure out where to get started, this guide will help communities identify tools that offer coherent and concise guidance that translates complex resources into action-oriented strategies and tactics.

WHAT IS THE PURPOSE OF THIS DOCUMENT?

US Ignite believes that each smart city device and network improvement can support residents in public spaces (e.g., severe weather events, mass casualty events, bad traffic, carriers of COVID-19, lawful protests) without compromising their personally identifiable information (PII) or losing the confidence that the public places in the municipality. Given the absence of universal policy practices and legal framework, this guide provides an accessible, actionable, procedural, and topical policy guide for municipal leaders to help them build better cities and communities. This guide offers clarity on key concepts, best practices, policies, examples, toolkits, and resources to help municipal leaders make informed decisions with respect to five policy domains: (i) Data Governance; (ii) Cybersecurity; (iii) Privacy; (iv) Community Engagement; and (v) Equity.

This guide has been prepared in consultation with subject matter experts and municipal leaders to:

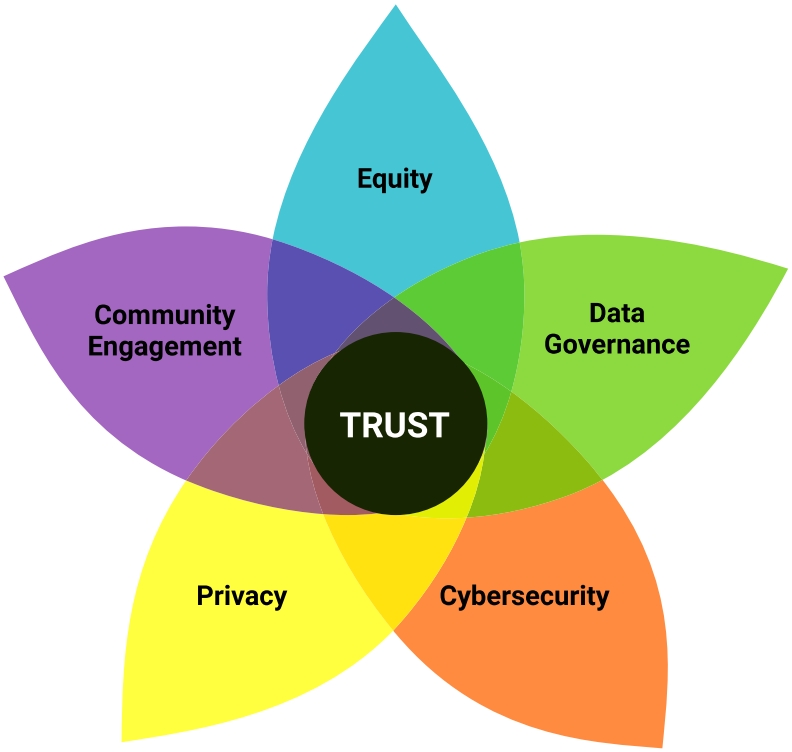
- Provide clarity on key concepts and roles encouraging cities and communities to establish a shared vocabulary.
- Help cities establish internal controls, policies, and practices across the five policy domains.
- Enhance decision-making by addressing critical policy considerations related to smart city applications.
- Provide resources that municipal leaders can use for training, discussion, and decision-making purposes.

1 CISA. (2020. January). Trust in Smart City Systems Characteristics and Key Considerations. https://www.cisa.gov/sites/default/files/publications/Trust%20in%20Smart%20City%20Systems%20Report_0.pdf

WHY THE FIVE POLICY DOMAINS?

Cities and Communities spend too much time and resources on smart and connected community projects without fully committing and thinking through policy issues that are essential for fostering civic trust. Civic trust is central to the smart city movement as it is both the end and the means to a successful smart city project. The five policy domains discussed in this guide overlap and interact with one another, and together they are critical to fostering civic trust for smart city projects. As cities and communities deal with these five policy issues they face indecision and poor decision-making due to a lack of resources, expertise, regulations, and governance frameworks.

FIG 1. ECOSYSTEM OF CIVIC TRUST



Source: Author.

WHO SHOULD USE THIS GUIDE?

If you are a leader or an employee at a large, small, medium, rural, urban, or suburban city or community that is becoming more smart and connected, or in a community on the outside looking in to see where data can help, this guide is for you. This guide has been created explicitly for cities and communities in the early stages of policy maturity, network deployments, and technology adoption and integration.

HOW SHOULD WE USE THIS DOCUMENT?

The guide provides a framework to facilitate discussions and decision-making. The best practices outlined in this guide are agnostic of technology types and apply broadly to smart city applications. Cities and communities should think about the policies - within each policy domain - that apply to a specific use case, given the city's jurisdiction and nature of smart city application they are considering. The resources provided in the guide reflect only a subset of the thousands of valuable resources. These resources are not an endorsement, but a selection of comprehensive and readable documents that can augment the decision-making process and provide guidance on the next steps.

HOW IS THIS GUIDE STRUCTURED?

This guide's structure sets it apart from the already existing guides and documents. Each section is dedicated to a specific policy domain, is self-sufficient, and can be read in parts. This guide meets you where you are in your journey. Each section is accompanied by an overview at the start of each section to help you navigate right to the issue that presents the most potential risk or confusion to your city or community.

DATA GOVERNANCE

CYBERSECURITY

PRIVACY

COMMUNITY ENGAGEMENT

EQUITY

“BEING ABLE TO DEMONSTRATE EFFECTIVE OWNERSHIP AND STEWARDSHIP OF DATA ELEMENTS IS KEY TO DATA GOVERNANCE.”

– NATHAN SNYDER
PARTNER AT BRICKENDON CONSULTING

SECTION 1

DATA GOVERNANCE

1. DATA GOVERNANCE OVERVIEW

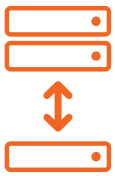
"Why do we care?" about data governance and some key concepts to get started.

Data Strategy & Policy for Good Data Governance – Section 1.1

- Data strategy & why it's needed (1.1.1 – 1.1.2)
- Examples of data strategy (1.1.3 – 1. 1.4)
- Data policy & why it's needed (1.1.5)

Key Aspects of Data Governance – Section 1.2

- Identify what's collected (1.2.1)
- Create data inventories (1.2.2)
- Assigning roles and responsibilities (1.2.3)
- Classify data (1.2.4)
- Define data access (1.2.5)
- Ensure data quality (1.2.6)
- Data retention & destruction (1.2.7)
- Preserve data (1.2.8)
- Use data efficiently (1.2.9)
- Ensure data oversight (1.2.10)



Key Considerations for Data Sharing – Section 1.3

- Data sharing & integration (1.3.1)
- Risks & benefits of data sharing (1.3.2)
- Role of data professionals in data sharing (1.3.3)
- Types of data sharing agreements (1.3.4 - 1.3.5)
- Responding to data requests (1.3.6)
- Data de-identification (1.3.7)
- Prepare a successful data request (1.3.8)

Understanding Open Data – Section 1.4

- Open data & its guiding principles (1.4.1)
- Move to open data (1.4.2)
- Draft your open data policy (1.4.3)

Check out the resource repository at the end of the section.

1. DATA GOVERNANCE

WHY DO WE CARE?

Cities and communities generate data by monitoring an array of activities, including pedestrian and vehicle traffic monitoring, waste and air quality management, and many other use cases. Data collection and management forms the basis of smart city applications. As such, a city or a community's success depends on how well it uses its data to improve residents' and visitors' experiences.

Data Governance is often used as a catch-all term to define how data are collected, stored, protected, used, and shared. For our discussion, we define data governance as the implementation and enforcement of a set of policies and practices to manage and use data so that cities and communities can extract maximum value from it to provide a better quality of life to its residents and organizations.

Data governance's goal is to break information silos, harmonize data systems and practices, and create a data-driven organization. As cities ramp up the utilization of data to make decisions regarding delivering public goods and services, it becomes critical to institutionalize data practices, policies, and roles that guide how the data is managed and shared.

Good data governance is essential for creating well-functioning, sustainable, and innovative smart cities and communities. In this section, we discuss the following:

1. Establishing a Data Strategy and a Model Policy for Good Data Governance
2. Key Aspects of Data Governance
3. Key Considerations for Data Sharing
4. Understanding Open Data
5. Data Governance Resource Repository for Cities and Communities

KEY DEFINITIONS:[1]

- **Administrative Data** – Data which is derived from the operation of administrative systems (e.g., data collected by government agencies for the purposes of registration, transaction and record keeping, which is then used for business and statistical purposes).
- **Dataset** – A particular collection of data, curated for a specific purpose or classification. Data Assets – Data collected and/or sourced and stored by an organization.
- **Data Classification** - A way to group a set of related categories in a meaningful, systematic, and standard format based on their sensitivity level.
- **Data Management** – The practice of collecting, keeping, and using data securely, efficiently, and cost-effectively with the goal to maximizing benefits to the organization.
- **Data Sources** – A place or system or service where data are obtained.
- **Metadata** – It is data that provides information about one or more aspects of the data.

1 Oracle. (n.d.). Data Management. Retrieved April 2021, from https://www.oracle.com/database/what-is-data-management/#link1 ; Government of New Zealand. (n.d.). Data Capability Framework Guide. Data.Govt.Nz. Retrieved April 2021, from https://www.data.govt.nz/manage-data/data-capability-framework/data-capability-framework-guide/#Glossary ; NIST. (n.d.). Computer Security Resource Center. Retrieved April 2021, from https://csrc.nist.gov/glossary.

1.1. ESTABLISHING A DATA STRATEGY AND A MODEL DATA POLICY FOR GOOD DATA GOVERNANCE

1.1.1 WHAT IS A DATA STRATEGY?

A data strategy is a comprehensive vision document that guides the city or community's goals, policies, practices, and principles. It outlines how to optimally use data to maximize the value of the city or community and the people it serves.

1.1.2 WHY SHOULD CITIES AND COMMUNITIES HAVE A DATA STRATEGY?[2]

Regardless of the size of the city or a community, a formalized and well documented data strategy creates the foundation of a shared vision and can help unlock the strategic benefits of using data to make better decisions that can efficiently deliver public goods and services.

TIP: CHECKLIST FOR CREATING A DATA STRATEGY

- Set your vision (Refer to pg. 7 of Data Governance Playbook)
- Assess your data maturity (Refer to pg. 9 of Data Governance Playbook)
- Establish data principles (Refer to Federal Data Strategy principles or DOD's principles or FAIR principles for data management)
- Define your goals
- Implement timelines, metrics, and data practices (Refer to pg. 13 of Data Governance Playbook)

1.1.3 WHAT ARE SOME GOOD EXAMPLES OF A DATA STRATEGY?

Some prominent data strategies from federal agencies, state and local governments include:

- **Federal Data Strategy** – includes a 10-year roadmap for federal agencies. It has four components that provide guidance for federal data use and management. The document includes a mission statement, 10 timeless principles, 40 practices to operationalize the principles, and 20 action steps to implement the practices.
- **Department of Defense (DOD)'s Data Strategy** – outlines DOD's vision, focus areas, and eight guiding principles for all their data efforts. The strategy also identifies four essential capabilities needed to achieve the agency's seven goals which include making the data visible, accessible, understandable, linked, trustworthy, interoperable, and secure.
- **California's Data Strategy** – outlines the mission and vision for the state of California. It further provides three goals and 10 objectives to empower state agencies to use data to make better decisions.

2 Government Chief Data Steward. (2018, December). Data Strategy and Roadmap for New Zealand [Slides]. Government of New Zealand. https://www.data.govt.nz/assets/Uploads/data-strategy-and-roadmap-dec-18.pdf

1.1.4 WHAT IS A DATA POLICY? HOW IS IT DIFFERENT FROM DATA STRATEGY?

A data policy outlines the basic principles, tasks, and procedures regarding proper data handling and data lifecycle management. It also attempts to define the roles and responsibilities of data management to help cities and communities think through their data policies and staffing.

QUESTIONS TO CONSIDER

- What outcomes are you trying to achieve?
- How will the data help to meet organizational needs?
- How are you going to track, monitor, and assess the implementation of the strategy?
- How will you communicate the strategy with the staff and stakeholders?

TABLE 1. DIFFERENCE BETWEEN DATA STRATEGY AND DATA POLICIES

DATA STRATEGY	DATA POLICIES
Data Strategy provides an overarching vision and plan for the entire organization.	Data Policies provide more granular details about how the data will be handled across the organization.
It is not legally binding.	It can be legally binding if properly and formally adopted.

QUESTIONS TO CONSIDER

- Who should be involved in the process of creating a data policy?
- How will the policies be communicated to all stakeholders?
- If policies are not legally binding, how will they be enforced?

1.1.5 WHY A DATA POLICY IS NEEDED?

A set of institutionalized data policies help to create: (i) consistent access to data across agencies; (ii) consistent storage format, structure, and vocabulary; (iii) clarity of roles and responsibilities; (iv) shared and open flow of information; (v) clarity about what data are collected and by whom; and (vi) proper attention to privacy, access, and retention.

TIP

Refer to US Ignite's Data Standards and Policies database for municipal data policies.

Also, refer to the recently published white paper on Smart City Data Governance Policies for recommendations on how to create policies for digital transformation and data sharing needs for the future.

1.2. KEY ASPECTS OF DATA GOVERNANCE

You cannot govern data when you don't know what data you have and who has access to it. Therefore, the bare minimum of data governance is to identify what your organization is collecting, identifying who is responsible for storing it or owning it, and giving them specific responsibilities and guidelines.

1.2.1 HOW CAN CITIES AND COMMUNITIES IDENTIFY WHAT DATA ARE BEING COLLECTED?[3]

One of the very first steps toward good data governance is identifying what is being collected. This means that cities and communities should create a data inventory or a data catalogue. This process can be broken into three steps:

DEFINITION

A data inventory is a list of datasets that provides descriptions of the type of data, their source, frequency, unit of measurement, and other useful information. They are closely related to data dictionaries.

FIGURE 1. CREATING A DATA INVENTORY

Source: Modified based on DataSF.

1.2.2 WHY SHOULD CITIES AND COMMUNITIES CREATE DATA INVENTORIES?[4]

A data inventory offers the following benefits:

- They ease the discovery process and make it easy to locate and use data as and when needed.
- They eliminate redundancies and duplication of efforts by identifying what is collected.
- They improve data quality as well as decision making.

TIP

- Looking for a data dictionary template? Refer to this data dictionary template by U.S. Department of Agriculture or refer to this data inventory template by DataSF.
- Refer to pg. 6 of DataSF guidebook and refer to this step by step guidance to create a data inventory depending on the complexity level of your preference (see pg. 4). A one page summary of the data inventory process can be found here. Alternatively, refer to this white paper on how to create a data inventory or you can also refer to guidance for creating data dictionaries from the Government of New Zealand.

3 DataSF. (n.d.). Data Coordinator Guidance. Retrieved April 2021, from https://datasf.org/resources/data-inventory-guidance/
4 Ibid.

1.2.3 WHAT ROLES AND RESPONSIBILITIES SHOULD BE ASSIGNED?[5]

Several key roles help maintain good data practices. These roles represent a set of responsibilities that individuals must address while managing data, particularly while sharing data between teams or with other cities and communities. Individuals in smaller cities and communities may take on the mantle of more than one role but thoughtfully defining how each role is addressed is critical for robust data governance. Have at least one individual with technical and analytical data skills and one with an understanding of the business side of data use.

TIP

Refer to CDO Playbook by Deloitte Insights and Beeck Center.

TABLE 2. ROLE AND RESPONSIBILITIES FOR DATA GOVERNANCE

ROLE	DESCRIPTION OF RESPONSIBILITIES
Chief Data Officer (CDO)	Designated by a municipal executive, the CDO is accountable for the overall implementation and reporting of the data strategy and policies.
Data Steward	Data Stewards are in charge of individual databases, datasets, or information systems. In general, a data steward has business knowledge of the data and can answer questions about the data itself.
Data Custodian	Data Custodians assist with the technical implementation of individual databases, datasets, or information systems. Not all systems or data sources will have a data custodian.
Data Owner	The Data Owner is the ultimate holder of rights to data within the data store. In mixed data environments this may be several individuals. In cases of derived data, a clear chain of ownership should be established for data artifacts, data surrogates, and any synthesized data.
Data Producer	The Data Producers may be individuals, organizations, or even devices where data originates for the datastore.
Data Manager	The Data Manager, sometimes referred to as the "Data Executive", is responsible for ensuring an effective data plan, ensuring the clear identification of the other major roles, and what agreements and specific policies should be in place to manage data effectively.

Source: DataSF Guidebook.

Defining roles and responsibility is not an end itself. It is important to train employees regularly to keep them up to speed with the skills required to carry their responsibilities efficiently. For guidance on what skills are required and how to assess these skills, refer to the data skills catalog and the playbook on assessing data skills included in the Federal Data Strategy.

QUESTIONS TO CONSIDER

- How will the roles be formalized?
- What organizational changes are required to identify and establish these roles?
- How will the employees receive training for their roles?

5 Ibid.

1.2.4 HOW CAN CITIES AND COMMUNITIES CLASSIFY DATA?[6]

Data can be classified as having risk along two broad dimensions: operational and privacy. Operational risks impact business processes, products and services, and may carry a significant liability or cost with breaches or mishandling. Privacy risks include direct or indirect impacts on individuals or other organizations through identity theft, economic loss, humiliation or discrimination.

Data classification helps to understand how the information needs to be saved, used, protected and more importantly, decide who should and should not have access to it. Once a data inventory is created and roles and responsibilities are assigned, use the inventory to classify data as:

- **Public/ open (least sensitive)** – data that can be freely shared with everyone; alternatively, data that has negligible or insignificant impact on the city, community, and any individual if breached.
- **Private** – data that cannot be publicly shared but can be used by governments that have a low impact on the city, community, and any individual if breached.
- **Sensitive/Confidential** – data that is protected by law (for instance, health data), that if breached can lead to significant reputational and economic damage to the city or community, as well as individuals.
- **Highly Sensitive/Highly Confidential** – data that, if breached can severely impact a city or community's ability to perform its statutory functions.

TIP

Refer to D.C.'s data classification here.

TIP: TOP FIVE THINGS CITIES AND CONNECTED COMMUNITIES CAN DO TO GET STARTED:

1. Create a data inventory
2. Assign roles and responsibilities
3. Classify your data.
4. Identify who should and should not have access to the different classes of data.
5. Brainstorm how you can use data to meet your organizational need.

1.2.5 HOW CAN CITIES AND COMMUNITIES DEFINE DATA ACCESS?[7]

Data access is typically described in terms of permissions to access and permissions to work with data. Depending on the classification of data, cities and communities should decide who gets access to which levels of data. Use the principle of least privilege to determine who gets access and how much control they have over the data or system. The principle states that any person or system should have the least access to data that will allow them/it to fully carry out their tasks and responsibilities. Learn more about the principle and review some examples here.

CAUTION

Classifying data can be tricky as some datasets may be deemed open by federal or state laws such as voter registration data. However, there is always a risk that even after removing all elements of personally identifiable information it can be traced back to an individual.

6 US Ignite (n.d.). Model Data Governance Policy. (Internal policy document); DigitalGuardian. (2016). The Definitive Guide to Data Classification [Slides]. Infosec. https://infosecpartners.com/wp-content/uploads/2017/02/The-Definitive-Guide-to-Data-Classification.pdf

7 Ibid.

Data access permissions are typically described in terms of what functional actions users with data access may take. Typically, these fall into four main categories:

- **Read-Only** – Users have access to view but not modify or change any data.
- **Limited Read-Only** – Users have access to read portions of the data from derived views or other restricted system tables.
- **Modify Data** – Users have permission to edit or modify existing data but not create new data.
- **Creation** – Users have permission to create new records or data fields within the datastore.

QUESTIONS TO CONSIDER

- Is the data complete?
- Are there any errors or missing values in the dataset?
- What is its unit and itsfrequency? Is it consistent across data points?
- Are there any inconsistencies across data sources?

1.2.6 HOW CAN CITIES AND COMMUNITIES ENSURE THE QUALITY OF DATA?[8]

Data quality ensures the overall health, utility, and trustworthiness of managed data. It refers to a series of attributes that ensure data can be effectively used. This includes formats, validation, encodings, accuracy, completeness, consistency, and standards that affect how reliably and easily data can be manipulated and used. It can be defined as:

TIP

Refer to this data quality module by preparecenter.org

Data Quality = Completeness of Data x Validity of Data x Timeliness of Data

Regular data quality checks can help organizations understand their data sources and potential sources of error in their data and develop a mitigation strategy accordingly.

1.2.7 WHAT IS DATA RETENTION AND DESTRUCTION?

An important aspect of data governance is to define data retention and destruction policies. Depending on the nature and legal requirements around data, cities and communities should decide how long it is justifiable to hold on to data (refer to the resource repository for resources on data retention guidelines).

Provide a clear guideline and timeline on how and when the data should be destroyed and disposed of, consistent with any applicable federal or state laws at the end of the retention period. In the case of data shared with a third party, it is absolutely critical to validate that the data has actually been deleted as per the terms and conditions of the data sharing agreement. Ask for proof to verify data deletion by the third party.

TIP

Refer to NIST's guideline for Media Sanitization. It provides guidance for four levels of sanitization – refers to removing information such that recovery is not possible – including Simple Disposal, Clearing, Purging, and Destroying.

8 DAMA UK Working Group. (2013, October). The Six Primary Dimensions for Data Quality Assessment. DAMA UK. https://damauk.wildapricot.org/resources/Documents/DAMA%20UK%20DQ%20Dimensions%20White%20Paper2020.pdf; Dasy Center. (n.d.). Data Governance Toolkit: Data Quality. Retrieved April 2021, from https://dasycenter.org/data-governance-toolkit/data-quality/

1.2.8 HOW CAN CITIES AND COMMUNITIES PRESERVE DATA IN CASE OF AN EQUIPMENT FAILURE, NATURAL DISASTER, OR CYBERATTACK?[9]

Floods, fires, viruses, ransomware, and hacks can destroy digital data or render it inaccessible. Periodic data backups of all data and systems should be mandatory. Data backup creates a duplicate copy of the data in a secondary location. As such, data backup is critical for preserving data in an event of equipment failure, natural disaster, or a cyberattack (read the Cybersecurity section of this guide to learn how to protect your data, networks and systems from a cyberattack).

Cities and community leaders should decide what type of backup they want to do, how often they want to do backups and how they want to do backups. The Resilient Organization guide by TechSoup is a three-part guide - Disaster Preparedness, Disaster Recovery, and Staff Preparedness – that provides best practices and steps to prepare and plan for natural disasters and cyberattacks. The three-part guide is written for non-profits but can come in handy for cities and communities that are just getting started. Refer to the guide based on what you need to know:

QUESTIONS TO CONSIDER

- How much data to backup and how often?
- What devices and applications should be used for backup?
- How would you ensure the security of sensitive backup data?
- How will you keep track of the backup records?

TABLE 3. OVERVIEW OF TECHSOUP GUIDES

GUIDE	WHAT CAN YOU EXPECT TO LEARN?
Disaster Preparedness	• Why is disaster preparedness important and how can we assess where you stand and what you need to do next? • How can we create a disaster preparedness plan, principles of technology disaster planning and backup solutions and strategies? • How can we inform and train your staff, and handle employee transition?
Disaster Recovery	• How can we activate our recovery plan and reestablish internal and external communications? • How can we recover data, systems, and equipment?
Staff Preparedness	• What communication tools can be used? • How should we develop and periodically review the disaster management plan? • How can we prepare an emergency supply kit?

Source: Author based on TechSoup's Resilient Organization Guide.

9 TechSoup. (2020). Disaster Planning and Recovery Guide. https://www.techsoup.org/disaster-planning-and-recovery

1.2.9 HOW CAN CITIES AND COMMUNITIES USE DATA EFFICIENTLY?[10]

The first step to thinking about data use is defining the problem that the organization is trying to solve. There are several frameworks and principles (see resource repository) that provide guidance on how organizations can use data to drive maximum social value. Key principles to keep in mind for safe and effective use of data are:

- **Deliver Clear Public Value** – The use of data should deliver clear public value and benefit to municipal management and/or its residents, businesses, and other organizations. It should be used to meet the needs of the constituents and deliver public services efficiently and cost-effectively.
- **Ensure Data are Fit for Purpose** – Cities and communities may end up hoarding data that is not needed. Data stewards and managers should clearly define how the data serves a purpose and solves a problem.
- **Focus on People** – It is not the data but the people that cities and communities should aspire to protect. They should actively consider ways to prevent the misuse of information that can harm their residents.
- **Maintain Transparency** – As cities and communities ramp up the use of data, the key to maintaining trust is by engaging with stakeholders and communicating clearly how the data are being used to make decisions and how it impacts the lives of residents.
- **Forge Strategic Partnerships** – If your city or community is limited in its ability to use data because of lack of data skills, an alternative is to forge partnerships with nearby cities, communities, academic institutions, local non-profits and independent consultants and utilize their expertise. The Commonwealth of Virginia has a partnership with their technical college system where information system and computer science students intern for different state agencies in Virginia and build applications/platforms for the state as part of their coursework.
- **Understand Limitations** – Data can be a powerful tool for cities and communities. It, however, has its own biases and can lead to discriminatory or unbiased outcomes if not assessed properly. Refer to the Equity section of this guide to learn how to operationalize data use to achieve your equity goals.
- **Retain Human Oversight** – Given that biased data or data sources can lead to inequitable or discriminatory outcomes there is a need to avoid overreliance and dependence on data by adding a human in the loop to oversee final decision making.

QUESTIONS TO CONSIDER

- What is the problem that the organization is trying to solve?
- What data are needed to solve the problem at hand?
- How long does the data need to be retained?
- How will it be disposed after use?
- Who should be informed how the data are being used and how will the organization communicate the information?
- How and who to report to if there are errors or inconsistencies in data?

TIP

Refer to Federal governments Data Ethics Framework for guidance on ethical data use.

10 Government of New Zealand. (2018, May). Principles for the safe and effective use of data and analytics. https://www.stats.govt.nz/assets/Uploads/Data-leadership-fact-sheets/Principles-safe-and-effective-data-and-analytics-May-2018.pdf; New South Wales Government. (n.d.). Module 8: Data-driven Culture. Retrieved April 2021, from https://data.nsw.gov.au/data-governance-toolkit-0/module-8-data-driven-cultu

- **Establish Mechanisms for Reporting Errors and Inconsistencies** – Every employee at some point might be playing the role of a data steward. As employees work with city or community data, they should know "how" and "to whom" to report inconsistencies or errors in a dataset, who should have access, and their duty to report any loss or breach.
- **Foster a Data-Driven Culture** – Focus on fostering a work culture that values data as an organizational asset. Provide resources and learning opportunities to all employees. Design performance metrics or incentive structures to reward data-driven values and behavior. A change in work culture may be required to move the needle and introduce fundamental changes in how employees deal with data daily. Failure to do so is likely to result in data silos, data quality degradation, and sub-optimal data utilization.

1.2.10 HOW CAN CITIES AND CONNECTED COMMUNITIES ENSURE DATA OVERSIGHT?

While implementing a data strategy and a data policy are great steps towards establishing data governance, cities and communities need a data oversight board or a data advisory group to oversee data governance and decision making within the organization. This group should constitute a group of multi-disciplinary leaders from across the organization. It can also include external stakeholders to make the group more representative and inclusive. This group should be responsible for, but not limited to, defining success metrics, coming up with a communication plan, evaluating data-driven decision making, and advocating for a data-driven culture.

TIP

The oversight board should have the following representation:

- The CDO or equivalent
- Chief Information Officer or equivalent
- Data stewards and custodians
- Data analysts from different departments
- A member from city clerk's office
- City Manager or an administration officer
- A professor or an independent consultant with expertise in data science
- One or two members of the public with data skills

1.3. KEY CONSIDERATIONS FOR DATA SHARING

1.3.1 WHAT IS DATA SHARING AND INTEGRATION?

Data sharing is the practice of providing partners within and outside the organization access to information or data to facilitate learning and collaboration on shared priorities. It can multiply the value that cities and connected communities can extract from data. Data integration is a form of data sharing which refers to "the joining or merging of data based on common data fields. These data fields can include personal identifiers, such as name, birth date, social security number, or a common encrypted "unique ID" that is used to link or join records at the individual level."[11]

11 Actionable Intelligence for Social Policy. (2020, May). Introduction to Data Sharing & Integration. https://www.aisp.upenn.edu/wp-content/uploads/2020/06/AISP-Intro-.pdf

1.3.2 WHAT ARE THE RISKS AND BENEFITS OF DATA SHARING?[12]

Data sharing and integration has significant benefits as well as risks:

TABLE 4. RISKS AND BENEFITS OF DATA SHARING

BENEFITS	RISKS
Holistic view of data and information.	In the absence of proper safeguards, there is always a high risk of security breach when data are transferred.
Scalable data to make better decisions.	Since the data are shared and used by partners who may not be the original source of data there is a risk of data being misinterpreted especially in the absence of metadata.
It allows for data reuse that can significantly cut cost and save time spent to otherwise collect data to answer questions around implementation and evaluation of public services.	Sharing data can perpetuate and replicate structural racism and may misrepresent economically disadvantaged people who have historically been the target of discrimination.

[6] Source: Modified based on AISP.

1.3.3 WHAT ROLES DO DATA PROFESSIONALS PLAY IN DATA SHARING?

TABLE 5. DATA ROLES IN DATA SHARING AND WITHIN ORGANIZATION

	ROLE IN DATA SHARING	ROLE WITHIN ORGANIZATION
Chief Data Officer or equivalent	Oversees the process and defines the terms for data sharing agreement.	The overall leader for data governance.
Data Owners	Accountable for the quality and security of the data and holds decision-making authority regarding access and use.	Typically, agency leadership with signatory authority.
Data Steward	Responsible for the governance of data, including metadata. Support established processes and policies for access and use.	Typically, the subject matter experts and data analysts that work with data.
Data Custodian	Responsible for the technology used to store and transport data.	Typically, an IT person or team.

Source: Modified based on AISP.

12 Ibid.

1.3.4 WHAT ARE DATA SHARING AGREEMENTS?

When sharing data between individuals or organizations, it is important to have an explicit agreement that outlines acceptable policies for use, privacy, handling, breach or loss reporting, and other concerns to set the appropriate expectations, and ensure proper handling. Refer to the Contracts for Data Collaboration library for a list of data agreement examples by sector.

Elements of a good data sharing agreement address:

- **Limited Data Set Definition** – This details the collections, types, and formats of data to be shared. This not only helps maintain an understanding of what is visible to all parties but serves as an important check on whether data is being inadvertently shared.
- **Safeguards for Handling, Access and Storage** – This includes expected measures for preventing breaches, exposure, and basic access to data. It may include requirements for encryption at rest and during transfer, securing endpoints, restricting access and other important security or integrity procedures.
- **Passthrough Requirements** – This should explicitly require disclosure of any additional agencies or individuals who may obtain access, including subcontractors. It should detail the need for any additional notification procedures and processes (including training) to ensure they abide and agree to all requirements of the data sharing agreement, and explicitly define additional agreements required.
- **Data Risk Assessment** – Assessment of risk of exposure of data, what the impact might be and to whom. See data classification for different data based on their operational and privacy risk levels.
- **Confidentiality and Privacy** – This should detail any requirements to protect individuals or any Personally Identifying Information (PII) within the dataset. This may range from a simple agreement not to share or expose data, to an agreement that requires the modification of data to de-identify individuals and what level they must do it. Refer to the Privacy section of this guide to learn more about privacy.

QUESTIONS TO CONSIDER

- Why do we need to share the data?
- Who are the stakeholders involved and who should be informed about data sharing?
- What type of data are being shared?
- With whom is the data being shared?
- How will it be shared?
- Is it legal to share the data?
- Is the data sharing ethical?

TIP

Refer to this playbook on how to draft a successful Memorandums of Understanding and Data-Sharing Agreements.

1.3.5 WHAT ARE THE DIFFERENT TYPES OF DATA SHARING AGREEMENTS?[13]

TABLE 6. TYPES OF DATA AGREEMENTS

AGREEMENT TYPE	BEST FIT FOR	SPECIFICS
Memorandum of Understanding (MoU)	• Ongoing data transfers with consistent and formalized parameters. • When the basis of a relationship is grant funding or a service contract.	• Roles and responsibilities of involved groups. • Why agreement is required. • Terms and conditions of partnership.
Data Use Agreement (DUA)/ Data Use Licenses (DUL)	Individual data sharing transactions.	• Parameters for data transfer. • Access information. • Intended data use. • Time parameters for data use. • How the requester should destroy the data.
Enterprise Memorandum of Understanding(E-MOU)	Long term agreement signed by multiple parties (for instance government agency to government agency) to facilitate multiple data sharing requests.	• Describe parties involved. • Set up governance boards. • Define codified request procedures. • Responsibilities of data stewards and data requesters.
Data Sharing Agreements (DSA)	Long term data sharing relationships that involve multiple transfers with different parameters.	• Identify the involved parties. • Terms and conditions for the partnership. • They can stand independently or be an addendum to an MOU or E-MOU. • May also define a process for authorizing data requests along with requirements for storing, protecting, and disposing of shared data.
Business Associate Agreement (BAA)	Personal Health Information.	• Each parties' responsibilities.
Statement of Work (SOW)	To provide a detailed overview of the project in all its dimensions.	• Information about vendors and contractors who are bidding to work on the project. • Timeline & Deliverables. • Scope of Work. • Budget.
Non-Disclosure Agreement (NDA)	Binding contract between two or more parties that prevents sensitive information from being shared with any others.	• Parties involved. • Laws governing the NDA. • Information that is being declared as confidential.

Source: Modified based on Skylight's Data Sharing Playbook.

13 Skylight. (n.d.). Data Sharing Playbook. Retrieved April 2021, from https://skylight.digital/work/toolkits/data-sharing-playbook/responding-to-data-requests/

1.3.6 HOW SHOULD CITIES AND COMMUNITIES RESPOND TO DATA REQUESTS?[14]

Cities and connected communities can have data sharing relationships within their organization, with other government organizations, with external companies/vendors or with the public. Which agreement an organization uses depends on the nature of sharing and parties involved. Some agreements can also be used together, for instance Enterprise Memorandum of Understanding (E-MOU), Data Sharing Agreement (DSA) and Data Use Agreement (DUA) are often signed together. The organization must work closely with its legal team to ascertain if a data agreement is needed in the first place. For instance, sharing open access data does not require an agreement. If an agreement is needed, they must decide which agreement is best suited to protect the interest of the organization and the people they serve.

TIP

Consider setting up a data request process to streamline how your organization responds to data requests. Steps to get started:

- Set up a request form/questionnaire.
- Create and publish a data dictionary.
- Data request fee (if applicable)

1.3.7 HOW CAN WE APPROACH DATA DE-IDENTIFICATION/ANONYMIZATION FOR RESPONDING TO DATA SHARING REQUESTS?

De-identification/anonymization refers to the process of removing all personal identifiers from data. Lack of legal frameworks around de-identification of data, inconsistency in understanding and lack of clarity on what constitutes as a personally identifiable information makes de-identification all the more difficult and challenging. The following are the primary steps to approach de-identification/anonymization of data:

- **Identify Who will Lead the Process** – Identify who the request should be directed to and who will work closely with the requester to analyze how the data needs to be de-identified. Typically, the data steward or the data owner of the dataset is in the best position to understand the request and direct it through its due process.
- **Who Else Should be Involved in the Process** – Establish a process that involves permission from all the relevant stakeholders. These stakeholders include, but are not limited to, the CDO, legal team, communications team, data analysts, and the administrative staff handling the data. Approvals from all stakeholders should be documented before initiating the de-identification process.

QUESTIONS TO CONSIDER

- Who works with the requester to understand the de-identification needs of the data requested?
- Who should be involved in the request approval process?
- What's the cost involved in the de-identification process? Who pays for it?
- Is it acceptable to refuse requests on the grounds other than confidentiality of data?
- How will the organization document the provisions of de-identified data to the requester?
- Consider what other documents maybe needed (eg. MOU, DSA, etc.)?

14 Ibid.

- **Grounds for Approval** – Authorize the data stewards or owners to reject a request on the grounds of confidentiality, risks, time and cost, as well as the purposes of the requester.
- **Consider Centralized De-Identification Services** – Create a centralized de-identification service where a team of technical experts can take the lead on all de-identification requests. In the absence of in-house expertise, cities and communities must consider onboarding independent researchers or partnering with data science departments at local academic institutes.

1.3.8 HOW CAN WE PREPARE FOR A SUCCESSFUL DATA REQUEST?[15]

Cities and communities may also find themselves in a position where they have to request data from external parties (government organization or a vendor). That is when having a plan for creating a data request will come in handy. Consider including the following in your plan:

- **Problem Statement** – A description of the problem that you hope to solve with the data. Refer to Bardach's 'Define the Problem' section.[16]
- **Identify the Data** – This is where published data inventories/ dictionaries come in handy. Review the data inventory of the organization and identify the data you need to meet your objective.

TIP

Follow these steps to get organized before you approach a data owner with a data request.

- **Establish credibility** – Outline how the partnership with the organization will help you address the problem at hand. Provide information on how you plan to use, protect, share (internally), and store data.
- **Make the Case for Data Sharing** – Highlight how the data owner can benefit from data sharing. Identify and emphasize if there are any potential synergies from the collaboration.
- **Specify the Parameters of Data** – The more specific you are the easier it will be for others to process your request. Provide information on the specific date range, frequency, unit or specific filters such as age, gender, geography, etc.
- **Provide a Realistic Scope and Timeframe** – Give the data owner a reasonable timeframe to consider and complete your request. Keep in mind the time needed to draft and sign a data sharing agreement.

15 Ibid.
16 Eugene Bardach (2012), A Practical Guide for Policy Analysis – The Eightfold Path to More Effective Problem Solving, Fourth Edition, Sage, Los Angeles.

1.4. UNDERSTANDING OPEN DATA

1.4.1 WHAT IS OPEN DATA AND WHAT ARE ITS GUIDING PRINCIPLES?

Open data refers to data that can be freely used, reused, and distributed to the public. This implies that data should be both legally open – placed in public domain for use with minimal restrictions – as well as technically open – published in an electronic machine readable and non-proprietary format.[17]

TIP

Refer to the list of definitions for Open Data concepts.

There are several (such as the International Open Data Charter and Sunlight Foundation's 10 Principles for Opening Up Government Information) open data principles that form the foundation for open data access and sharing. Broadly speaking, open data are based on the principles of open by default, availability and access, reuse and redistribution, universal participation, comparable and interoperable, and inclusive development and innovation.

1.4.2 HOW CAN CITIES AND COMMUNITIES START TO OPEN UP DATA?[18]

- **Identify Data Coordinators** – The first step to building an open data program is identifying the data champions across different departments who are skilled and, in a position, to make a commitment to open data. Cities and connected communities should designate "Data Coordinators" for each department who will act as the main point of contact and accountability for open data in their department. Data Coordinators will take the lead in developing inventories for the department, establishing timelines for publishing, implementing privacy, data licensing, metadata and other data practices.
- **Start Simple and Small** – There is no harm in starting small and simple. Even publishing just one dataset or subset of a larger dataset is a great start. Cities and communities should focus on small wins of high value and build on them and multiply wins over time.
- **Choose your Dataset(s)** – This is one of the most critical steps in opening up data. Having a pre-existing data inventory can make this step relatively easy. Once the organization has a data inventory they should:
    - Consult with all stakeholders (in-house data professional, data governance board members, and the public) to understand which dataset(s) will create the most social value if published.

17 World Bank. (n.d.). Open Data Essentials. Retrieved April 2021, from http://opendatatoolkit.worldbank.org/en/essentials.html
18 Open Knowledge Foundation. (n.d.). Open Data Handbook. Retrieved April 2021, from https://opendatahandbook.org/guide/en/how-to-open-up-data/

- Undertake a risk-benefit analysis to weigh the benefits of releasing the data against the privacy risks it may pose to the organization or an individual. Open data are likely to conflict with individual privacy as organizations mature and add more data to their open data platforms, and therefore each dataset is assessed to ensure that it has been de-identified before being shared openly. Assessments such as the benefit-risk analysis undertaken by Future of Privacy Forum to evaluate City of Seattle's Open Data Risk Assessment are good examples for cities and communities to follow.
- Other than the risk, cities and communities may also consider data which are the easiest to release.
- Open data has become a cornerstone for the smart city's movement. Cities and communities can always learn from the roll out of datasets of cities that have a well-established open data program (refer to resource repository).

TIP

Refer to this de-identification protocol for open data.

- **Apply an Open License** – A critical step to make data legally open is to specify a license. The Federal Open Data Policy states: "Agencies must apply open licenses, in consultation with the best practices found in Project Open Data, to information as it is collected or created so that if data are made public there are no restrictions on copying, publishing, distributing, transmitting, adapting, or otherwise using the information for non-commercial or for commercial purposes." Examples of open licenses and dictation can be found here.
- **Make the Data Technically Open** – The data should be available in an electronic machine-readable format. Cities and communities can host data on their website or via third party sites.
- **Post the Applicable Open License and Any Appropriate Metadata and Disclaimers** – Appropriately describing the dataset, its content, metadata, applicable licensing, and any legal disclaimers is important. If the data are not real-time, the snapshot time should be included.
- **Make it Available and Discoverable** – Post a data inventory on the data portal that users can browse through or preview without downloading the dataset. Be thoughtful about the user-friendly format(s) in which the data can be downloaded to maximize the utility that users can get from the dataset.

TIP

- Refer to common license types for datasets here.
- Local libraries and academic institutions' digital libraries, arXiv.org, and GitHub are open-access repositories that cities and connected communities can use to host their data. For instance, City of Boston launched its Open Data to Open Knowledge project in collaboration with Boston Public Library.

- **Engage and Get Feedback Early and Often** – Engage with potential and actual users in the early stages of development of the program. Get feedback on dataset and data formats that will be of most value to them. Open data is an iterative process, and their feedback can help organizations make sure that the next round of iterations fill the gaps identified in the first round of datasets released.
- **Periodic reports on Progress in Implementing Data** – Lastly, the Chief Data Officer (CDO) or equivalent should provide periodic reports or updates on the progress and implementation of the open data program. The report should outline datasets opened overtime, plan for future data releases, and feedback and evidence from stakeholders on the usability and relevance of open data.

1.4.3 WHAT IS AN OPEN DATA POLICY AND HOW CAN CITIES AND CONNECTED COMMUNITIES DRAFT AN OPEN DATA POLICY?

An Open Data policy provides information on what data will be made public and how it will be made public. It is a testament to a city's commitment to transparency and innovation. The Open Data Policy Hub by the Sunlight Foundation provides a collection of 109 local and 12 state governments open data policies.

There are many resources available to help cities and communities craft their open data policies. A report by the National League of Cities analyzed open data policies of five cities and provided recommendations on how cities can achieve their goal of open data. The Sunlight Foundation provides detailed guidance on establishing open data and offers a policy generator tool to help cities and communities craft their own open data policy.

1.5. DATA GOVERNANCE RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		DATA STRATEGY AND FRAMEWORK	
1	The 5 Essential Components of a Data Strategy	Intermediate	Written for for-profit organizations, the report explains why a data strategy is important. It introduces the five key components of a good data strategy.
2	Data Management Strategy 2019-2022	All	A simple easy to read and visually appealing data strategy from the City of Dallas.
3	Oregon's Data Strategy 2021 – 2023	All	A draft of Oregon's data strategy was published for public comment in July 2020. The document captures the guiding principles, outcomes and a roadmap for action to achieve its data goals.
4	Data Ethics Framework (Government of U.K.)	All	An ethics framework for data use developed by the government of the United Kingdom. The framework includes the principles and self-assessment frameworks for actions.
5	Ethics & Algorithm Toolkit	Intermediate – Advanced	A toolkit developed for governments to assess the risk of data-based decision making.
6	The Data Equity Framework	All	This seven-step framework is easy to apply and doesn't require you to reinvest the way your team works. It helps you apply the equity lens by offering simple steps and checklists to apply the tool.
		DATA INVENTORY & RETENTION	
7	Retention Schedules for Local Governments: Five Things You Should Know	All	Read tips on retention schedule based on North Carolina's new General Records Schedule for Local Government Agencies.
8	Guide to the Inventory, Scheduling, and Disposition of Federal Records	All	This guide provides essential information, guidance, and tools necessary for Federal agency records managers to establish, manage, and operate an effective records disposition program within their agencies.
		DATA SHARING	
9	Sharing Data for Social Impact: Guidebook to Establishing Responsible Governance Practices	Beginner – Intermediate	A comprehensive guide that captures the different aspects of data sharing including: (i) defining and understanding the data being shared, understanding ethical implications of data sharing; (ii) defining operations, formalizing best practices, drafting data sharing agreements; and (iii) driving impact, monitoring and assessing privacy and security concerns, and processes to improve data quality.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
10	Smart Cities Data Sharing Framework	Intermediate – Advanced	The report discusses the role of data sharing in smart cities, business opportunities, trends in industry approaches, introduces a data framework and concludes with recommendations for city planner on next steps for supporting city's data evolution plan.
11	State of Connecticut Data Sharing Playbook	All	A great resource for local government to get started with data sharing. It also provides examples and further recommended readings on the different steps involved in data sharing.
12	California Health and Human Services (CHHS) Data Sharing Framework	All	Refer to the example of process flow, legal agreement, form and instructions provided by CHHS.
13	Using and Sharing Data/ National Association of Counties	All	A great resource for examples, workshops, reports and toolkit for data sharing and use.
	DATA DE-IDENTIFICATION		
14	Data De-Identification Guidelines	Advanced	This resource from CHHS provides guidance on de-identification methods, examples, reporting types and legal frameworks.
	OPEN DATA		
15	A De-identification Protocol for Open Data	All	The blog published by International Association for Privacy Professionals (IAPP) provides five step guidance with examples to data de-identification for open data.
16	City of Seattle Open Data Policy	All	A good example of open data policy if you are looking for examples to draft your own data policy.
17	District of Columbia (D.C.) Data Policy	All	D.C. has a comprehensive policy with its open data polices baked into its data policies.
18	Open Data	All	A great resource that provides background on open data and a model policy including examples and additional resources.
19	Chief Data Officer's Annual Report (D.C.)	All	A good example of a report by the CDO on the progress of the open data program.
20	City of Seattle Open Data Risk Assessment	All	A risk assessment of Seattle's open data program undertaken by the Future of Privacy Forum (FPF). The report discusses the different privacy risks tied to open data and provides a model for risk-benefit analysis for opening up data.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
21	City Open Data Policies	All	A great report from the National League of Cities provides an analysis of the open data policies of five cities – Chicago, Austin, Seattle, Boston, and Amsterdam. It concludes with recommendations based on the lessons learned from the implementation of the policy in the five cities.
22	Project Open Data Metadata Schema	Intermediate – Advanced	Provides guidelines and resources for data standards, open data as well as examples of data field and types.
23	OpenDataPhilly	All	The City of Philadelphia's open data program. Refer to the list of datasets offered by the city and the different formats in which it is offered.
24	Open Government	All	See the list of cities and counties with open data programs.
25	Open Data Privacy	All	The report is divided into four parts/chapters: (i) introduces the concepts and practices for doing a risk-benefit analysis of open data; (ii) outlines a lifecycle approach to managing privacy in open data; (iii) emphasizes role of internal control; and (iv) describes the role of public engagement.
26	Standard Open Data Licensing	All	A list of resources by DataSF on licensing open data. It provides recommendations on data licensing, inventory of licenses across cities and states, and a practical guide to licensing open data.

“CYBERSECURITY IS A SHARED RESPONSIBILITY, AND IT BOILS DOWN TO THIS: IN CYBERSECURITY, THE MORE SYSTEMS WE SECURE, THE MORE SECURE WE ALL ARE.”

– JEH JOHNSON
FORMER UNITED STATES SECRETARY OF HOMELAND SECURITY

SECTION 2

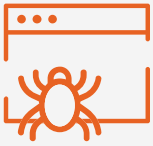
CYBERSECURITY

2. CYBERSECURITY OVERVIEW

"Why do we care?" about cybersecurity and some key concepts to get started.

Understanding Cybersecurity Governance – Section 2.1

- Cybersecurity governance & who should be involved (2.1.1 - 2.1.2)
- Information security policy & its importance (2.1.3)
- Draft your security policy (2.1.4)
- Frameworks & standards for managing cybersecurity risk (2.1.5)



Understanding Cyberattacks – Section 2.2

- Identify what's collected (2.2.1)
- Cyberattacks & cyberattackers (2.2.1 - 2.2.2)
- Types of cyberattacks (2.2.3)
- Stages of cyberattack (2.2.4)
- Cyber Boom Model (2.2.5)

Best Practices in Cybersecurity – Section 2.3

- Prevent & protect from cyberattack (2.3.1)
- During a cyberattack (2.3.2)
- After a cyberattack (2.3.3)

Check out the resource repository at the end of the section.

usignite

2.CYBERSECURITY

WHY DO WE CARE?

Cybersecurity is the risk management of a city or community's digital operations and data. *It refers to a set of practices, policies, and standards that can help prevent and protect against cyber incidents.* Effective cybersecurity measures lay the foundation for robust risk management, harmonize business processes, provide protection from potential civil and legal liabilities, assures security, policy compliance, and protects the trust and confidence of the public.

A cyberattack cost a city in Maryland over $18.2 million. The city officials were denied access to their computer networks for weeks and residents had to resort to mail-in and in-person visits to pay their bills. Later an audit report found that the city lacked appropriate cybersecurity measures to prevent the attack. This is just one example of the many cyberattacks that we have seen on local governments.

Local governments are easy targets as they: (i) are a treasure trove of personal data; (ii) often have outdated/legacy systems; (iii) are historically underfunded and understaffed; and (iv) customarily lack sufficient training in cybersecurity measures and defenses. Consequently, cyberattacks pose a major risk of irreversible damage to the city and community's assets and reputation.

Interestingly, cities and communities identify cybersecurity as their top priority but often fail to invest or allocate sufficient budget and resources for it.[2] A part of the reason is that cybersecurity has largely remained a very technical and inaccessible issue for city and community officials. This section aims to simplify the discussion of how cities and communities can take appropriate measures to address their cybersecurity concerns. We discuss the following:

1. Understanding Cybersecurity Governance
2. Understanding Cyberattacks
3. Best Practices in Cybersecurity
4. Cybersecurity Resource Repository for Cities and Communities

KEY DEFINITIONS:[1]

- **Adversary** – Individual, group, or organization that conducts, or has the intent to conduct, detrimental activities.
- **Application(s)** – System/function for collecting, saving, processing, and presenting data by means of a computer.
- **Computer System** – Also referred to as system; is a basic, complete and functional hardware and software setup with everything needed to implement computing performance.
- **Incident** – An adverse network event in an information system or network or the threat of the occurrence of such an event.
- **Legacy Systems** – An environment containing older systems or applications that needs to be secured to meet today's threats.
- **Malicious Code** – Software that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.
- **Network** – Two or more computers that are linked in order to share resources (such as printers), exchange files, or allow electronic communication.

1 Glossary of Security Terms. (n.d.). SANS. Retrieved April 2021, from https://www.sans.org/security-resources/glossary-of-terms/?msc=securityresourceslp; NIST. (n.d.). Computer Security Resource Center. Retrieved April 2021, from https://csrc.nist.gov/glossary/term/adversary.

2 Newcombe, T. (2021, April 23). Cybersecurity in 2019: A Time for Bigger Budgets and More Talent (Contributed). GovTech. https://www.govtech.com/opinion/cybersecurity-in-2019-a-time-for-bigger-budgets-and-more-talent-contributed.html

2.1. UNDERSTANDING CYBERSECURITY GOVERNANCE

2.1.1 WHAT IS CYBERSECURITY GOVERNANCE?[3]

Cybersecurity (also referred to as just security) governance refers to the business practices, processes and controls that are put in place to ensure organizational security and manage potential cybersecurity risks.[4] Even for cities and communities that outsource cybersecurity services, cybersecurity governance is important because outsourcing does not guarantee absolute protection.

Cybersecurity governance should include the following:

- Defining and assigning roles and responsibilities to security professionals who will play an active role in protecting the daily operations and resident privacy.
- Cybersecurity practices and processes that govern operations and protect critical assets.
- Code of conduct for employees for securing and protecting data and systems.
- Internal as well as external rules and regulations needed to ensure the integrity of systems, networks, and data (compliance requirements). Refer to the resource repository for a cybersecurity compliance guide.
- Guidelines to safeguard the reputation of the organization.

2.1.2 WHO SHOULD BE INVOLVED IN CYBERSECURITY GOVERNANCE?

The goal should be to build a multi-disciplinary team of:

- **Business Executives** – Individuals that are involved with the business side of operations. They can be department heads who ensure integration and cooperation of security practices with the operations of their department.
- **Chief Information Security Officer (CISO)** – Cities and communities may have a Chief Technology Officer (CTO), Chief Information Security Officer (CISO) or even an Information System Security Officer (ISSO). Regardless of the title, it is paramount to have a designated leader who will be responsible for overseeing all information security practices.

TIP:
CHARACTERISTICS OF AN EFFECTIVE SECURITY GOVERNANCE

- Applies to the entire organization.
- Holds leaders accountable.
- Clearly defines roles and responsibilities.
- Takes a risk-based approach.
- Complies with relevant requirements including laws, ordinance, and other organizational policies.
- Addressed and enforced in Security Policy.
- Commits and sets aside adequate budget/resources.
- Well communicated with staff and external vendors/partners.
- Reviewed and audited.

Source: Modified based on Educause.

TIP

- Refer to the guidance document on Information Security Governance for a list of questions to consider for successful implementation of Information Security Governance.
- Read about more about the role of a CISO here.

3 Educause. (n.d.). Information Security Governance. Retrieved April 2021, from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/information-security-governance
4 Ibid.

- **Information Technology (IT) Personnel** – Individuals directly involved in overseeing network and system operations and security.
- **Steering Committee** – A diverse group of individuals from across the departments as well as some external security experts responsible for addressing security concerns and creating accountability.
- **Cyber Incident Response Team** – In addition to these roles, build an exclusive cyber incident response team including lawyers, public relations (PR) professionals, and IT professionals who will be the first responders and firefighters during a cybersecurity incident.

TIP

Refer to Infocyte's practical guide to build your own cyber incident response team.

2.1.3 WHAT IS AN INFORMATION SECURITY POLICY AND WHY IS IT IMPORTANT?[5]

Information security policy is a set of rules, directives, procedures and practices that provide clear guidance on how the organization manages, protects, and shares information. The policy should concur with relevant laws, legislation, applicable standards such as the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) as well as other internal organizational policies that exist. Security policy is a critical aspect of security governance, and without it there is no mechanism to enforce standards and govern effectively.

TIP

For guidance refer to Information Security Policy of the following cities:

- San Jose
- New York
- Seattle

2.1.4 HOW CAN CITIES AND CONNECTED COMMUNITIES DRAFT A SECURITY POLICY?[6]

A well-designed security policy is implementable, enforceable, and easy to understand. It should include the following:

i. **Policy Rationale** – Clearly define why the policy is needed. This can include a business, legal or a regulatory rationale.

ii. **Scope** – Define who and to which systems the policy applies and clearly state any exceptions and exclusions that apply. The policy should be mandatory for everyone to whom it applies.

iii. **Policy Statement** – Describe expected outcomes and goals, and detail how employees should follow the policies in their work.

TIP

- Refer to 50 security policy templates provided freely by SANS to draft your own policy.

5 Educause. (n.d.-b). Security Policies. Retrieved April 2021, from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies

6 Ibid.

iv. **Roles and Responsibilities** – State who is responsible for enforcing the policy and monitoring its implementation. The policy can also define who is involved in security governance.

v. **Definitions** – Define any acronyms, jargons or words that may be ambiguous or may have different interpretations.

vi. **Related/Relevant Documents** – Include any related or relevant standards, frameworks, or policies that should be referred to in order to gain a thorough understanding of the policy.

vii. **Policy History (if any)** – Include reference to previous versions of policy (if any) and highlight all significant changes in the new policy vis-à-vis the previous version.

A comprehensive security policy can also include standards, procedure, and guidelines.

QUESTIONS TO CONSIDER

- Who should be consulted and included in the process of drafting a security policy?
- How will the policy be communicated with both internal and external stakeholders?
- How to make the policy enforceable?
- Who is responsible for enforcing the policy?

TABLE 1. STANDARDS, PROCEDURES, AND GUIDELINES

	ROLE	DESCRIPTION
Standards	Measurement (How much?)	Minimum action needed to comply with policies.
Procedures	Detailed Steps (How? When? Who?)	Detailed step-by-step checklists to perform a task.
Guidelines	Recommendations (What? How? When? Who?)	Advice and recommendations for employees to do their job appropriately in line with policies.

Source: Educause.

2.1.5 WHAT ARE SOME FRAMEWORKS AND STANDARDS FOR MANAGING CYBERSECURITY RISK?

There are several frameworks and standards that provide guidance on managing information security risk. Prominent ones include Minimum Safety Requirements for Federal Information and Information Systems (FIPS 200), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST Special Publication (SP) 800-37 Rev. 2), Center for Internet Security (CIS) controls, and Risk Management – Guidelines (ISO 31000:2018).

TIP

Refer to a list of cybersecurity standards here.

The NIST Cybersecurity Framework, when complemented with the NIST Risk Management Framework, provides the most comprehensive framework for cybersecurity risk management. The Risk Management Framework provides inputs and guidance on how to establish controls, standards and requirements to manage risk given the functions, categories, and sub-categories defined in the Cybersecurity Framework. Take into account the resources, culture, organization structure, and legal requirements when selecting a framework that works best for your organizational goals and needs.

TIP

Refer to GCTC-SC3 Cybersecurity and Privacy Advisory Committee Guidebook for step-by-step guidance on how to implement NIST Risk Management Framework.

CAUTION: GOVERNANCE AND MANAGEMENT SHOULD NOT BE CONFUSED. WHILE GOVERNANCE RELATES TO "DOING THE RIGHT THING", MANAGEMENT IS ABOUT "DOING THINGS RIGHT."

GOVERNANCE	MANAGEMENT
Oversight	Implementation
Authorizes decision rights	Authorized to make decisions
Enact policy	Enforce policy
Accountability	Responsibility
Strategic planning	Project planning
Resource allocation	Resource utilization

Source: Educause.

2.2. UNDERSTANDING CYBERATTACKS

2.2.1 WHAT IS A CYBERATTACK?

Cyberattack is defined as an "attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."[7] Cyberattacks can be grouped into un-targeted and targeted cyberattacks. The un-targeted cyberattacks target systems, devices, and users indiscriminately. A targeted cyberattack is where the attacker strategically singles out a system because they have some interest in the organization's business. Targeted attacks can be more dangerous as they may even extend to an employee's personal computer system, or those of family members.

7 NIST. (n.d.). Computer Security Resource Center. Retrieved April 2021, from https://csrc.nist.gov/glossary/term/Cyber_Attack

2.2.2 WHO ARE CYBER ATTACKERS?

Cyber attackers can be classified into four major groups based on their intent:

TABLE 2. TYPES OF CYBER ATTACKERS

TYPE	DESCRIPTION
Cyber Criminals	They usually target organizations, systems, or personal data that can be monetized on the dark web or controlled in demand for a ransom payment. They can indulge in sophisticated hard-to-discover attacks.
Hacktivists	They are individuals who perform the attack to reinforce their political, social or religious, or personal ideology.
State-sponsored Attacks	These are attacks carried out against a particular targeted country or its assets or interests, under the sponsorship of an adversary nation-state, where the attacker wants to create social, political, economic or military instability advantageous to the penetrating state.
Insider Threats	These are attacks carried out by someone with knowledge of and access to an organization's computer system, usually by virtue of employment or a working relationship with the targeted organization. Attacks can be from employees, vendors or external partners. The trust factor involved makes it hard to detect. They can be malicious, accidental or even a result of negligence.

Source: Appsealing.

2.2.3 WHAT ARE THE DIFFERENT TYPES OF CYBERATTACKS THAT CITIES AND COMMUNITIES SHOULD KNOW ABOUT?[8]

Cyber attackers are becoming more sophisticated and so are the types of cyberattacks. The two most common type of cyberattacks that every city and community employee should know about are:

- **Malware** – The term is used to describe a malicious code and includes ransomware, spyware, viruses and worms.
    - **Ransomware** is a form of attack where the adversary blocks access to key components of the network or system unless a ransom is paid. CISA's Ransomware Guide provides guidance on best practices for ransomware prevention and a checklist for ransomware response. Refer to a resource repository for a list of resources on ransomware.

TIP

Read about 10 most common types of cyberattacks of all times.

TIP

This two-hour interactive experience allows city officials and community members to learn what it takes to combat ransomware.

8 Cisco. (n.d.). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved April 2021, from https://tools.cisco.com/security/center/resources/virus_differences#3 ; Cisco. (n.d.-a). What are the Most Common Cyber Attacks? Retrieved May 2021, from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

- **Spyware** covertly extracts information. Read more about top 15 malicious spyware actions.
- **Viruses** as the name suggest are malicious codes that can spread from one computer to another from an infected host. It works by inserting a copy of itself into and becoming part of another program. The severity of the virus may range drastically from temporary effects to damaging data or software causing denial-of-service (DoS) conditions.
- **Worms** are much like viruses; they differ in that they can be standalone and do not need a host software to spread.

Other kinds of malware include Trojans Horses and Bots.

- **Phishing** – The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Phishing is an increasingly common cyberthreat and the easiest to prevent if employees are repeatedly trained to detect, avoid, and report it. Learn about different types of phishing attacks here.

TIP

Take the Jigsaw Phishing quiz to test if you can identify a phishing email.

Take Cisco's Phishing Awareness Quiz here.

2.2.4 HOW DO CYBERATTACKS WORK?

To defend better, it is important to understand the different stages of a cyberattack. The Cyber Kill Chain framework created by Lockheed Martin defines the different phases of a cyberattack – Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Actions on Objectives – knowing these stages can help in early identification and prevention of cyber incidents. For simplicity, these phases can be condensed into four primary stages.

DEFINITION

Vulnerability refers to weakness in an information system, security procedure, or internal control that could be exploited by an adversary.

TABLE 3. STAGES OF CYBERATTACK

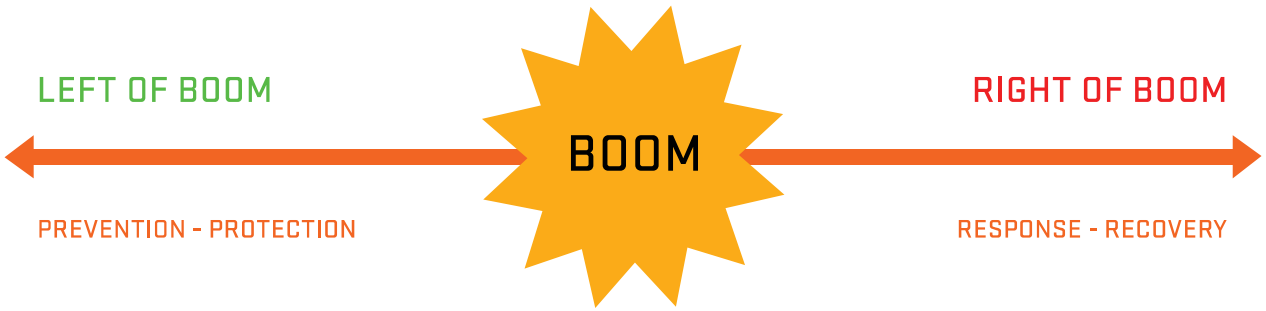
STAGE	DESCRIPTION
Survey	Investigating preliminary information about the target and potential vulnerability to design a plan for attack.
Delivery	Reaching to a point in a system or network where the vulnerability can be exploited.
Breach	Gaining unauthorized access by exploiting the vulnerability.
Affect	Meeting the goals of the attack by carrying out malicious activities or altering the system.

Source: National Cybersecurity Center, Government of U.K.

2.2.5 WHAT IS THE CYBER BOOM MODEL? HOW DOES IT HELP CITIES AND COMMUNITIES APPROACH CYBERSECURITY?[9]

Cybersecurity experts are increasingly using counter-terrorism models and strategies to prevent and protect against cyberattacks. A "cyber boom" refers to the time of the cyber incident; "left of boom" refers to events preceding the attack, and "right of boom" refers to events after the attack. This model provides a clear approach to cybersecurity measures for cities and communities by breaking down an incident into three phases.

FIGURE 1. CYBER BOOM MODEL



Source: Labor Relations Institute

- **Left of Boom** refers to the strategies that can be undertaken to prevent and protect against cyberattacks.
- **Boom** refers to the time when the cyber incident happens and is ongoing.
- **Right of Boom** is when the incident has happened, and the organization and authorities are assessing the damages. It refers to the strategies that can be undertaken to document the assessment, identify the cause and source of attack, repair or make up for the damage and learn lessons from what went wrong.

Part 3 of this section provides a litany of best practices that cities and communities should follow based on the three phases of the cyber boom model.

9 Nyotron. (2019, October 4). What is "Cyber Boom" and Why Should You Care? https://www.nyotron.com/what-is-cyber-boom-and-why-should-you-care/; Celaya, T., & Winkler, I. (2020, February 28). You Can Stop Stupid. RSA Conference. https://www.rsaconference.com/library/presentation/you-can-stop-stupid

2.3. BEST PRACTICES IN CYBERSECURITY

2.3.1 WHAT BEST PRACTICES CITIES AND COMMUNITIES CAN ADOPT TO PREVENT AND PROTECT FROM CYBERSECURITY INCIDENTS (LEFT OF BOOM)?[10]

- **Establish Cybersecurity Governance and Define Roles** – Much of the problem with cybersecurity is that cities and communities fail to document and communicate their processes, controls, and procedures properly. The first step to effective cybersecurity is to set up cybersecurity governance and define roles to create accountability.

- **Cybersecurity Assessment** – What is unknown cannot be protected. Cybersecurity risk assessments can help cities and communities identify vulnerabilities and risks across people, processes, systems, and vendors. The risk assessment should include:

    - *Asset management* – accounting for all the assets that are owned and should be protected by the city and community.

    - *Maturity assessment* – identify where the city or community is in terms of cybersecurity maturity and assess the gaps that need to be filled. Refer to the resource repository for a list of cybersecurity maturity assessment frameworks.

    - *Penetration testing* (pen test or ethical hacking) – a simulated authorized cyberattack on a computer system to evaluate the strength of the system security. For cities and communities that do not have in-house expertise, they can hire independent analysts or external vendors to undertake the assessment. Partnering with local academic institutions is also a cost-effective way to undertake cybersecurity assessment.

- **Awareness Training and Education** – Cybersecurity is everyone's responsibility irrespective of their role in the city or community. Cybersecurity is not a matter of "if" an incident occurs but rather "when" it occurs. Make cybersecurity awareness a part of all onboarding procedures. Provide regular training to every city employee and community member on good cybersecurity hygiene and how to detect and report potential cyberattacks. The primary goal of education and training should be to equip employees with the tools, information and controls needed to perform their duties safely.[11] Refer to the resource repository for a list of cybersecurity awareness and training resources available for cities and communities.

TIP

MIT has a public interest cybersecurity clinic that helps cities and towns with their cybersecurity vulnerability assessment.

TIP

Refer to these cybersecurity Dos and Don'ts!

10 Thompson, L. N. (n.d.). Cybersecurity Best Practices for Municipalities. New Hampshire Municipal Association. Retrieved April 2021, from https://www.nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities

11 Celaya, T., & Winkler, I. (2020, February 28). You Can Stop Stupid. RSA Conference. https://www.rsaconference.com/library/presentation/you-can-stop-stupid

- **Start with Small Steps** – The State and Local Government Security report found that most cyberattacks on state and local governments are not sophisticated and can be prevented by following simple cybersecurity practices. Some of these steps include:
    - **Move Beyond Passwords.** Passwords are passé. Passwords should indeed be strong but even strong passwords place too much trust in the users. As such, password use has largely been abandoned by non-password schemes such as Microsoft's login tools that leverage push requests to your phone. Make a move towards passwordless security—a form of zero trust. To get started read NIST's Zero Trust 101, read this guide on how to move beyond passwords, review these top 10 passwordless use cases and ask these top 10 questions to your potential passwordless provider/vendor.
    - **Two/Multi-Factor Authentication (2FA/MFA)** provides an additional layer of security. In addition, to a username and password, it requires additional information to log the user into their system or network. 2FA/MFA can prevent a cyberattack even if the password is guessed, leaked or hacked.
    - **Encryption** should be used to ensure the safety of all devices (computers, laptops, hard drives etc.) owned by the city or community. Full-disk encryption is used to protect "data at rest", it can be used to prevent data breach in case a device is lost or stolen. Refer to the resource repository for resources on encryption best practices.
    - **Regular Updates** are needed to maintain the security of all devices. Outdated systems expose a major vulnerability making systems prone to cyberattacks. System updates should be done routinely and made mandatory across departments. Applications that don't run after security updates should be updated themselves rather than indefinitely deferring updates.
    - **Regular Data Backup** is the best way to prevent data loss. A recent data backup can be a savior in the event of a ransomware attack. All systems and devices should perform routine backups of all files and data, and backups should be stored offsite to protect against loss of both the primary and backup information in case of fire or other disaster.

DEFINITION

Zero Trust is a security concept that requires all users, even those inside the organization's enterprise network, to be authenticated, authorized, and continuously validating security configuration and posture, before being granted or keeping access to applications and data.

TIP

Follow these best practices for data backup.

These steps if taken diligently can go a long way in preventing cyberattacks, mitigating potential damage in an event of a cyberattack and even bring about a change towards a culture of security.

- **Enforce Security Standards on Vendors and Others** – Cities and communities engage with external vendors to meet their organizational needs. When online and when communicating via email or other digital methods ensure vendors comply with the city or community's security protocols and enforce security requirements and standards applicable to the vendors. Perform thorough due diligence and assessment of all vendors who have access to confidential data or who interact with the city or community's systems and networks. Due diligence should include the evaluation of the tool or technology that the city or a community is procuring. The benefit of adopting a technology should be weighed against its cyber-risks. A report by the Center for Long-Term Cybersecurity ranked different smart city technologies based on their cybersecurity vulnerability to help local policymakers make decisions regarding technology adoption based on varying degrees of cyber-risk levels.

- **Known Mechanism for Reporting a Potential Cyberattack** – Inform employees how and to whom they should report a potential cybersecurity attack. For instance, if an employee receives an email that seems suspicious, they should know who to contact to verify the authenticity of that email and whom to report to in case it is in fact a phishing email.

- **Incident Response Planning** – Build a cyber incident response team who will act as first responders in the time of crisis. The team should have a response plan in place. To create a response plan, think through different threat scenarios and draft a chain of reaction that should be triggered to stop, mitigate, and address the attack. Moreover, know who should be informed in case of a breach, and who should you report to – police department, FBI, CISA, or some other federal agency – depending on the nature and magnitude of the attack. In case of a data breach, know which breach notification applies depending on the city or community's jurisdiction.

- **Cyber Insurance** – Allocate a portion of IT budget to cybersecurity depending on the size of the city or community. Use a part of this allocated budget to purchase cyber insurance to mitigate the economic cost that would be incurred in case of an incident.

TIP

Refer to New York City's Cybersecurity Requirement for Vendors & Contractors.

TIP

- Refer to Tabletop Exercises – Six scenarios to help prepare your cybersecurity team.
- Refer to data breach notification laws by state.
- Refer to CISA's guidance on reporting cyber incidents.
- Report a cyber incident to CISA.

TIP

Refer to this guidance from National Association of Insurance Commissioners (NAIC) for tips on purchasing Cyber Insurance Policy.

QUESTIONS TO CONSIDER

- Who should be consulted for cybersecurity assessment?
- What is the minimum level of cybersecurity training and awareness every employee should receive irrespective of their position and role?
- How to create a culture of cybersecurity?
- Who will undertake the vendor due diligence to ensure that the vendor complies with the security standards?
- How will security standards be enforced on vendors and external partners?
- Who is responsible for reviewing and documenting suspicious cyber activities reported by employees?
- Who should be informed about the incident?
- Where and how should the incident be reported?

2.3.2 WHAT ARE THE BEST PRACTICES DURING A CYBERATTACK (BOOM)?[12]

This is where the planning steps taken to the left of boom will come in handy. Once the attack has been detected the cybersecurity leadership should move fast to:

- **Contain** – If the attack is still on-going take immediate steps to contain it and take measures to mitigate harm. Shutting down networks and systems may save some of them.
- **Orient** – Identify the type of attack and ensure safety of employees, then data, and finally organization's reputation.
- **Prepare to Act** – Prepare to inform stakeholders, report the incident to concerned authorities, preserve evidence, and alert legal and PR team. This is where the incident reporting planning will help cities and communities move faster in the time of crisis.

TIP

Five to-dos to maintain reputation after cyberattack.

12 IBM. (2018). Beyond the Boom Improving decision making in a security crisis [Slides]. IBM. https://www.ibm.com/downloads/cas/BEGYVQZV

2.3.3 WHAT ARE THE BEST PRACTICES AFTER A CYBERATTACK (RIGHT OF BOOM)?

After the incident has taken place, prepare to respond and recover. These steps would include:

- **Act** – Inform stakeholders and report the incident to relevant authorities.
- **Document** – Identify the source and the timeline of the incident. Take stock of the damages. Hold people accountable for their mistakes by documenting the organizational, economic and social cost of the incident. Identify gaps in security procedures that led to the boom.
- **Initiate Recovery** – Undertake damage control with regards to the technical, economic, and reputational costs incurred by the organization.
- **Correct** – Focus on making corrections and remedying processes that created the vulnerability. Improve your cybersecurity standards, procedures, and practices based on the lessons learned from the incident. It is important to understand that cybersecurity is an iterative process, and no one gets it right all the time.

QUESTIONS TO CONSIDER

- Who should be involved in the documentation process?
- How will the costs be evaluated?
- How will the learning be communicated with the stakeholders?
- What needs to be changed, improved or eliminated to prevent a similar attack in the future?

If you want assistance, there are companies which specialize in cyberattack response. If you have a cyber insurance, you may want to take specific steps. It will be beneficial to know whom you plan to engage in case of a cyberattack before it happens.

2.4. CYBERSECURITY RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		CYBERSECURITY COMPLIANCE	
1	Cybersecurity Compliance: A Comprehensive Guide	Beginner	A simple guide to understand cybersecurity compliance. It describes the regulatory, legal and security controls to ensure the integrity of data, systems and networks.
		RANSOMWARE	
2	A Starting Point for Smart Cities and Communities on Managing Ransomware Risk	Beginner – Intermediate	A great easy to read paper that explains ransomware and associated risks and consequences. It also discusses consideration for planning, controls, and training.
3	Ransomware Protection Plan	Beginner – Intermediate	A short four-page document that provides tips for protecting and preparing against ransomware.
4	Securing Data Integrity Against Ransomware Attacks	Intermediate – Advanced	This NIST document provides guidance to prepare organizations to address any future data incidents.
5	FBI's Ransomware Guidance	All	FBI's guidance on ransomware prevention and what to do in event of an attack.
		CYBERSECURITY MATURITY ASSESSMENT	
6	Security Maturity Self-Assessment	All	A guide from Contra Costa County Employment & Human Services. It helps to quantitatively assess your current level of cybersecurity measures.
7	SIMM 5300-C – Cybersecurity Maturity Metrics (XLSX)	All	Cybersecurity Maturity Assessment from the California Department of Technology. Read more about how they developed the metrics here.
		TRAINING AND AWARENESS	
8	SANS Security Awareness Kit	All	A comprehensive kit from SANS with templates for security awareness program charter, annual program scheduler, presentation slides, phishing planning guide, work from home deployment kit and a program planning kit.
9	Security Infographics	Beginner – Intermediate	A collection of over 56 easy to read infographics that can be used for awareness training and security education.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
10	National Cybersecurity Awareness Month (NCSAM) Resource Kit	All	A list of resources for cybersecurity awareness. It also explains what the NCSAM is and why is it important.
11	Rochester Institute of Technology (RIT)	Beginner	RIT provides posters and videos for security awareness training.
12	List of Glossaries	Beginner	Refer to this resource for a list of glossaries that explains security and privacy terms and concepts.
13	Cybersecurity: A Social Engineering Approach at MIT	All	A cybersecurity clinic at MIT that helps cities and nonprofits with their cybersecurity assessments as well as provides resources for training and education.
14	CISCO Phishing Awareness Quiz	Beginner	Use this quiz to test employee's awareness of phishing.
15	Cybersecurity for Critical Urban Infrastructure (Course on edX)	Beginner – Intermediate	A course to prepare city officials, agency staff and a new generation of students seeking to serve as cybersecurity consultants to understand, help prevent and manage cyberattacks on vulnerable communities across America.
16	CISA – Stop.Think.Connect	All	List of resources and tips from CISA to increase understanding about cyberthreats.
		ZERO TRUST	
17	10 Tips to Enable Zero Trust Security	All	Read Microsoft's top 10 tips for zero trust security.
18	Getting Started with Zero Trust – Never Trust Always Verify	Intermediate – Advanced	A white paper that explains the concept of zero trust, how it works, its challenges, and the different stages involved in laying the foundations for zero trust security.
		ENCRYPTION	
19	Best Practices Encryption	Intermediate – Advanced	This short document provides guidance on three best practice encryption approaches.
20	Operation Best Practices for Encryption Key Management	Intermediate – Advanced	This resource from CISA discusses six key management use cases and provides guidance on encryption best practices.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		INCIDENT PLANNING AND RESPONSE	
21	Cyber Incident Response	All	A list of resources from CISA on cyber incident response. It provides guidance on how to report cyber incidents to the federal government and training for incident response.
22	Sensitive Data Exposure Checklist	All	A template that can be used to document the data exposed in an event of a cyber incident.
23	Data Incident Notification Toolkit	All	Templates for notifying data incidents.
24	AT&T's Insider's Guide to Incident Response	All	A comprehensive guide from AT&T on how to prepare your incident response team, response processes and procedures and tools for response.
		MISCELLANEOUS	
25	Cybersecurity Resources for Local Governments	All	A compilation of information security resources available to local governments in Washington State.
26	Protecting Our Data: What Cities Should Know About Cybersecurity	All	A report by the Nation League of Cities presents results from a survey on cybersecurity preparedness of cities. The report discusses policy landscape and resources of local governments and provides examples and recommendations for local leaders.
27	NIST Small Business Cybersecurity Corner	All	A list of resources provided by NIST for small business which can also be used by local governments for education and training purposes.
28	Michigan Cyber Partners	All	A partnership between various divisions at the State of Michigan, including Michigan Cyber Security and the Michigan State Police, and local public entities across Michigan to strengthen, improve, and promote cybersecurity resources and best practices.
29	Cybersecurity Planning Guide/ Federal Communications Commission	Beginners	This simple easy to read guide provides best practices, resources and examples for information security practices.

“PRIVACY IS NOT AN OPTION, AND IT SHOULDN’T BE THE PRICE WE ACCEPT FOR JUST GETTING ON THE INTERNET.”

– GARY KOVACS
FORMER CHIEF EXECUTIVE OFFICER OF AVG TECHNOLOGIES

SECTION 3

PRIVACY

3. PRIVACY OVERVIEW

"Why do we care?" about privacy and some key concepts to get started.

Create Privacy Principles & Policies – Section 3.1

- Privacy principles and why you should adopt one (3.1.1 – 3.1.2)
- Prominent privacy principles (3.1.3 – 3.1.4)
- Examples of privacy principles (3.1.5)
- Difference between privacy principles & policies (3.1.6)
- Dos and don'ts for privacy principles (3.1.7)

Create Accountability – Section 3.2

- Privacy professionals and why you need them (3.2.1)
- Hold your team internally accountable (3.2.2)
- Establish external accountability (3.2.3)

Evaluate Privacy Risk – Section 3.3

- Embed privacy into your procurement processes (3.3.1)
- Follow best practices and resources on assessing & monitoring privacy risks across activities (3.3.2)
- Overcome the challenges of limited resources and expertise (3.3.3)

Check out the resource repository at the end of the section.

usignite

3. PRIVACY

WHY DO WE CARE?

At its core, privacy is a fundamental human right that refers to as an individual's right to determine how their personal information is collected, used, and shared. Difficult to operationalize, privacy is dynamic, multi-faceted, and a highly subjective concept to understand.

Privacy concerns have taken center stage with the surge in data breaches, purposeful and unintentional misuse of personal information, and adoption of surveillance technologies and smart city applications. The continuous evolution of new technological capabilities has been accompanied by increased public scrutiny and awareness. As a result, we see cities and communities being increasingly concerned about the potential privacy risks and liabilities.

The severe public backlash that smart city projects have faced in recent times is a testament to how the relentless pursuit of smart city projects without due consideration of the unintended consequences to resident privacy can lead to privacy events that undercut public trust in municipal leaders and governments. The privacy risks grow exponentially as cities and communities evolve and collect more data on their residents, and use cases support the integration of this information across activities. Therefore, it is wise to place privacy at the forefront as cities and communities mature with regards to both policy and technology adoption.

In this section we provide best practices and guidance on:

1. Establishing Privacy Principles and Policies
2. Creating Accountability for Privacy
3. Evaluating Privacy Risks
4. Privacy Resource Repository for Cities and Connected Communities

KEY DEFINITIONS:[1]

- **Data Minimization** – The idea to collect and retain personal data necessary to inform a decision.
- **Disclosure** – A statement that provides details on how an organization will collect, process, use, and share individual data.
- **Informed Consent** – Unambiguous, specific, and informed indication, by a statement or by a clear affirmative action, that a person is agreeing to provide their personal data as well as grant permission for processing of their personal data as stated in the signed statement.
- **Privacy Event** – The occurrence or potential occurrence of problematic data actions.
- **Personally Identifiable Information (PII)** – Data or any element of data that can be used to establish or trace the identity of the person.
- **Social License** – Ongoing approval or broad social acceptance of a project within the local community and among its stakeholders.

1 (i) National Institute of Standards and Technology (NIST). (2020, January). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. NIST. https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf#page=32; (ii) What is the social license? (2020). SocialLicense.Com. http://socialicense.com/definition.html

3.1. ESTABLISHING PRIVACY PRINCIPLES AND POLICIES

3.1.1 WHAT ARE PRIVACY PRINCIPLES?[2]

Privacy principles are a set of standards or guidelines (binding or non-binding) intended to act as an overarching philosophy for the protection of the personal information of individuals collected, held, and used by government authorities and their stakeholders.

3.1.2 WHY SHOULD CITIES AND COMMUNITIES ADOPT PRIVACY PRINCIPLES?

Documenting and codifying privacy principles can help cities and communities achieve multiple goals:

- **Establish public trust** – The principles can serve as a testimony of a municipality's willingness to take responsibility and act in the best interest of resident privacy and security.
- **Align siloed departments** – The principles can serve as a north star for guiding the implementation of privacy practices across departments that may have a different understanding of privacy.
- **Create a culture of privacy** – The principles are aspirational in nature. They form the basis for everyone to carry out their responsibilities by creating a shared vision for embedding privacy in their daily operations.

3.1.3 WHAT ARE SOME OF THE PROMINENT PRIVACY PRINCIPLES?

There are several privacy principles available that can provide a starting point for coming up with a city or community's privacy principles. The following two sets of principles taken together are comprehensive and representative of the most commonly adopted privacy principles across the public and private sectors.

- **Organization for Economic Cooperation and Development (OECD)'s Fair Information Practice Principles (FIPPs)** - FIPPs were among the first internationally recognized privacy principles that served as privacy guidelines for the public and the private sectors across countries. Since then, the eight specific principles have evolved and have been infused into the privacy framework of several national and state governments around the world.
- **Privacy by Design** – The foundational principles of a framework (see 3.1) that bakes in privacy into an organization's design and operations of the IT system, network, infrastructure, and business practices with seven founding privacy principles.

2 Clopton, R. (2021). Effective Privacy Management in Local Government. Berkeley Public Policy Journal, Spring, 66–79. https://bppj.berkeley.edu/spring-2021-journal/

FIG 1. FIPPS AND PRIVACY BY DESIGN

FIPPS	PRIVACY BY DESIGN
• Collection Limitation • Data Quality • Purpose Specification • Use Limitation • Security Safeguards • Openness • Individual Participation • Accountability	• Proactive not reactive—preventative not remedial • Privacy as the default setting • Embed privacy into design • Retain full functionality (positive-sum, not zero-sum) • Ensure end-to-end security • Maintain visibility and transparency —keep it open • Respect user privacy—keep it user-centric

Source: Author based on FIPPS and Privacy by Design

3.1.4 WHAT ARE THE KEY CONSIDERATIONS AND COMMON THEMES THAT ARE PRIMARILY ADDRESSED IN PRIVACY PRINCIPLES?[3]

The most common considerations and themes that emerge in the privacy principles adopted by organizations across public, private, and non-profit sectors are as follows:

TABLE 1. COMMONLY ADDRESSED PRIVACY CONCEPTS

PRIVACY CONCEPT	DESCRIPTION
Accountability	Who should be accountable for breaches of responsibility and trust? How should accountability be ensured? What does accountability look like?
Accuracy	How should data be maintained in its most accurate form? Is the information fit for the use to which it will be employed?
Equity	How can the data be collected and analyzed responsibly so that it does not discriminate or mistreat information from vulnerable populations in a biased manner to exploit or harm vulnerable populations directly or indirectly?
Ethics	How can the moral obligation to evaluate the risks to individual privacy of any practice that collects and uses information be upheld?
Informed Consent	How will individuals be informed about how their information will be used and be provided with an option to deny collection or use of data?
Limiting Collection/Retention	How can we ensure that only the specific information required to provide services is being collected and stored only for as long as it is needed?

3 Clopton, R. (2021). Effective Privacy Management in Local Government. Berkeley Public Policy Journal, Spring, 66–79. https://bppj.berkeley.edu/spring-2021-journal/

PRIVACY CONCEPT	DESCRIPTION
Managing Data/Stewardship	How will the information be protected and stored in a manner that prevents unauthorized access?
Public Record Disclosures	How will we ensure individual privacy when responding to requests for public records while still complying with regulations governing requests?
Review of Systems	How and who will review current and future information systems and evaluate their potential impacts on the privacy of individuals?
Third Party Access	How and who will monitor interactions with third parties, including limiting access to information where possible and requiring third parties to comply with privacy principles?
Transparency	How can we ensure that the public is aware of what information is collected, how it is used, and who may have access?

Source: Modified based on Clopton (2021).

Of these eleven considerations: (i) Accountability, (ii) Informed Consent, (iii) Limiting Collection/ Retention, (iv) Third Party Access and (v) Transparency are among the most common and recurring for principles adopted by local governments.

3.1.5 ARE THERE ANY GOOD EXAMPLES OF CITIES OR COMMUNITIES THAT HAVE ADOPTED THEIR OWN PRIVACY PRINCIPLES?

At least seven local governments have adopted privacy principles in the past five years. Seattle did so in 2015, followed by Kansas City in the same year. Since then, several jurisdictions have adopted privacy principles, including Portland (2019); San Jose (2019); Oakland (2020); Mesa, AZ (n.d.); and New York City (2021).

It is difficult to pick one as the best. To some extent, they are all a work in progress and will need updating over time. However, if you are looking for a starting point, see principles from Seattle, Oakland or Portland. Refer to the resource repository for some more examples of privacy principles and to learn more about how these cities developed and implemented their privacy principles.

QUESTIONS TO CONSIDER

- What public value does your organization want to create through the principles?
- Who should be involved in the process of drafting the principles?
- Who should vet and approve the principles?
- Who will be responsible for implementing the principles?
- How will we communicate the principles to the residents and to the employees?
- Is there organizational support for the principles and the resource necessary to implement?

3.1.6 HOW ARE PRIVACY PRINCIPLES DIFFERENT FROM PRIVACY POLICIES?

Cities and communities may choose to incorporate their privacy principles within their privacy Policies or they may decide to keep them separate. The City of New York has a comprehensive Citywide Privacy Protection Policies and Protocols which provides a detailed description of its privacy practices and policies.

TABLE 2. PRIVACY PRINCIPLES V/S PRIVACY POLICIES

PRIVACY PRINCIPLES	PRIVACY POLICIES
Principles guide values for the entire organization.	Policies are internal statements that governs an organization or entity's handling of personal information. They direct members of the organization who might handle or make decisions regarding the personal information, instructing them on the collection, use, storage and destruction of the data, as well as any specific rights the data subjects may have and may also be referred to as a data protection policy.[5]
They are generally not legally binding and are meant to be aspirational in nature.	They are legally binding.

Source: Author.

3.1.7 WHAT ARE THE DOS AND DON'TS OF CREATING A PRIVACY POLICY?

DOS

- Follow applicable rules and laws - check for local rules that may particularly apply to your jurisdiction.
- Make it easy to opt-out of data collection.
- Make sure that the privacy policies are easily accessible on your website.
- Make sure the privacy policies align with data governance practices.
- Restrict activities to those that support use case.
- Make sure that policies and practices are documented, and sufficient training is provided to understand them.

TIP

Find out about the privacy law(s) in your state using International Association of Privacy Professional (IAPP)'s State Comprehensive - Privacy Law Comparison tracker.

5 International Association of Privacy Professionals (IAPP). (n.d.). Glossary of Privacy Terms. IAPP. Retrieved April 2021, from https://iapp.org/resources/glossary/#paperwork-reduction-act-2

DON'TS

- Don't use technical or legal jargon.
- Don't miss important clauses. Be very specific and provide details on any exclusions that may apply.
- Don't write long blocks of text.
- Don't use inconsistent policies across departments.
- Don't update privacy policies without notice.
- Don't assume you know what your community expects.

CAUTION: PUBLIC RECORD ACT (PRA), OPEN DATA AND PRIVACY

- PRAs vary from state to state. Some states may favor open data over privacy. This leads to a conflict as open data can have a lot of information being collected that could reveal individual identities or behavioral patterns that can have significant impact on groups and individuals. Furthermore, collection of different datasets can introduce new privacy challenges even if the individual datasets are anonymized.
- This inconsistency from state-to-state leads to gaps in judicial understanding. For instance, date and place may not be considered personally identifiable information (PII) in one state but it can be PII in another state.

QUESTIONS TO CONSIDER

- Who should be involved in the process of drafting the policies?
- How will you ensure that all practices have been disclosed correctly?
- Is the disclosure policy in alignment with Public Records Act (PRA)?
- Who will be responsible for enforcing and updating the policies?
- How will we obtain a clear agreement/ informed consent to privacy policies for residents?
- How will we communicate the privacy policies to the residents?

TIP

Still confused about PII? Refer to this guidance on PII by U.S. Department of Labor.

3.2. CREATING ACCOUNTABILITY FOR PRIVACY

Creating accountability by deploying safeguards both internally and externally is needed for operationalizing privacy principles and policies across all departments of a city or community.

3.2.1 WHAT IS THE ROLE OF PRIVACY PROFESSIONALS IN CREATING ACCOUNTABILITY INTERNALLY?

A number of cities and communities are hiring a dedicated Chief Privacy Officer (CPO) to oversee the privacy and data protection practices. This practice runs parallel to the Privacy Act of 1974 that requires federal agencies to have a privacy officer as well as the private sector practice to appoint a CPO. Having a dedicated CPO is a good practice because: (i) it creates accountability and a clear line of authority by having a dedicated position for privacy; and (ii) it sends a signal that the organization cares about privacy and thus strengthens public trust. If you cannot hire a CPO, consider existing job functions most impacted by privacy risk where the initial privacy approaches can be applied.

DEFINITION

Accountability is one of FIPPs principles' that pertains to a data controllers (cities and communities) responsibility to comply with measures which gives effect to its privacy principles.

TIP

See how Department of Homeland Security (DHS) describes the authorities and responsibilities of the Chief Privacy Officer here.

3.2.2 WHAT ARE THE KEY CONSIDERATIONS FOR CREATING INTERNAL ACCOUNTABILITY?[6]

- **Awareness and Transparency** – Information silos are commonplace across departments in cities and communities. Early communication and awareness training can help to harmonize privacy practices across departments. This includes engaging with department heads and employees early in the process to get their buy-in on privacy practices.
- **Identifying a Line of Authority** – A top-down approach requires establishing a chain of command to provide a shared vision and disseminate resources to those who are not familiar with the privacy practices. This would also depend on where the office of CPO is housed within the organization. The most common departments for a privacy office are Information Technology (IT), Human Resource (HR), and Legal.
- **Creating a Culture of Privacy** – Privacy should be fostered as a culture and value to conduct the day-to-day operations of the city or community. Creating a culture requires more than appointing a CPO. Cities and communities should nurture privacy champions within each department to facilitate awareness, training, and reinforcement of privacy principles to create a shift in culture and attitude towards privacy practices.

QUESTIONS TO CONSIDER

- Which department will house the office of the CPO or a lead privacy professional?
- What will the chain of command look like depending on where the office of CPO is housed?
- What should be the medium (complaint line, email, portal, etc.) for reporting potential privacy risks or concerns?

6 Flores, A., Sharma, J., Yeung, L., Clopton, R., & Miyano, S. (2020, May). Oakland Resident Data: Understanding What's Collected and Strengthening Privacy. Oakland Privacy Advisory Commission.

- **Training** – The privacy world is constantly evolving which makes training crucial to keep employees abreast with all the changes. Cities and communities should allocate budget for training; however, to get started, they can benefit from the many open-source resources available on privacy. Refer to the resource repository for resources on privacy.

- **Mechanism for Escalation and Red Flagging** – Tied to training is the need for creating a clear mechanism for escalation of potential privacy events. Employees should be trained to identify and report privacy risks and harm. While training will help employees identify potential privacy risks and breaches, having a mechanism for escalation and reporting will bring the matter in front of privacy professionals responsible for ensuring resident privacy.

CAUTION

Privacy risks are different from privacy harms. Risk is related to both the likelihood and impact of a privacy event whereas harm only relates to potential damages resulting from a privacy event.

3.2.3 WHAT ARE THE KEY CONSIDERATIONS FOR CREATING EXTERNAL ACCOUNTABILITY?[7]

- **Privacy Remedy and Redressal** – The vacuum of laws and rules around privacy makes it challenging for cities and communities to tackle remedies for privacy harms. As such, cities and communities should think beyond the legal requirements and proactively consider the consequences of a privacy event. An ombudsperson role is one interesting way to think about complaint lines for citizens to be heard, to make corrections, and access as well as delete their data. To this end, cities and communities should create a channel for residents to directly question the handling of their data. This has been a trend in the private sector, and it shouldn't be too long before people ask local governments (cities and communities) for the same. This goes hand-in-hand with the need for creating an internal escalation mechanism for reporting to ensure a feedback loop is in place to keep a check on privacy events.

- **External Oversight** – Accountability does not necessarily lead to trust when it is purely internal. Therefore, an external oversight is needed to keep a watchful eye. This can be done either through dedicated privacy advisory boards or city councils. This may also include engaging with local academic institutes and independent privacy researchers to conduct privacy evaluation and assessments. Annual reports and/or periodic assessments (triggered by material changes in organization or technology) and making them publicly available can go a long way in establishing transparency and accountability.

QUESTIONS TO CONSIDER

- How can we evaluate scenarios of what happens in case of individual privacy violation?
- How will we inform the residents in case of a breach?
- What corrective actions should be undertaken in case of a privacy event?
- Who will take corrective actions?
- What is at stake in case of a privacy event?

TIP

Refer to this model legislation from Oakland to form your own Privacy Advisory Commission.

7 Based on interviews with privacy experts.

TABLE 3. EXAMPLE OF STAKEHOLDERS ON A PRIVACY OVERSIGHT BOARD

CHIEF PRIVACY OFFICER (CPO)/ PRIVACY HEAD
Head of the Department leading the project
Representative(s) from a local or regional entity such as non-profits, faith-based organization
Representative(s) from academia
Representative(s) from the communications team
Representative(s) from vendor/private sector player

Source: Author.

3.3. EVALUATING PRIVACY RISK

Cities and communities should proactively assess privacy risks. Cities and communities should undertake risk assessments before as well as after the implementation of a smart city project. This section discusses: (1) how cities and communities should engage with vendors before adopting a smart city application; and (2) how cities and communities can evaluate privacy risks after the deployment of a smart city project.

3.3.1 WHAT CAN CITIES AND COMMUNITIES DO TO EVALUATE TECHNOLOGY SOLUTIONS OFFERED BY VENDORS?

Cities and communities are becoming increasingly dependent on external vendors as they digitize and adopt smart city solutions. City and community leaders should hold the vendors to the same or even higher standards of privacy as they hold themselves.

- Role of Due Diligence – Establish requirements for due diligence for vendor assessments, audits and identify who might have downstream access to data to ensure the data stays in safe hands. Be curious and ask the right questions, not stopping at the first answer, laying out requirements clearly, and being good consumers and skeptics of information making decisions in the public interest. City and community leaders should understand what the technology is, what it's capable of, who it impacts, its limitations and safeguards needed to limit potential harm. Refer to IAPP's privacy vendor list for a directory of companies that can help you protect data, provide services, meet regulatory requirements, respond to breaches, set policies and more.

QUESTIONS TO CONSIDER

- What problem is the organization trying to solve?
- What data needs to be collected?
- Is the data collection justified?
- Can data collection be minimized?
- Who ensures data is in safe hands?
- Does the vendor have experience deploying the proposed solution?
- How will the vendor transfer knowledge to the city or community employees?
- Do you have the social license to implement the technology (such as facial recognition)?

TIP

Refer to the checklist created by the International Association of Privacy Professionals (IAPP) for expedited vendor privacy and security assessment.

8 Read the foundational principles of Privacy by Design in Section 1.3.

- Privacy by Design – Privacy by design is a popular framework used by the private sector as an efficient and cost-effective way to safeguard privacy[8]. Privacy by design has a lot in common with the principle of minimization. It requires understanding and limiting the collection of data to what is truly needed to accomplish a set of goals. Cities and communities should establish a tangible connection between what is being collected, how it is being collected and how it will be used. Ask your vendor if they comply with principles of privacy by design (see 1.3) or with National Institute of Standards and Technology (NIST)'s privacy framework. Request proof of compliance with the framework, if required. There are two arguments for baking in privacy by design for smart city applications:
    - **Business Rationale for Collecting and Retaining Data** – We have learned from city records management processes that it is costly to hold data. The cost is both in terms of storage as well as the enormous liability tied to the risk of personal data breaches. A caveat here is that there are some laws or rules that may require some departments to retain data for certain periods of time.
    - **Building Better Tools and Developing Better Projects** – Privacy by design allows organizations to consider tradeoffs between potential risks and benefits from data use and address the burning questions regarding privacy upfront. This can save cities and communities a lot of time and resource that they would otherwise spend on building a use case.

TIP

The National Institute of Standards and Technology (NIST)'s Privacy Framework, though designed for the private sector, could be a key steppingstone for many jurisdictions to evaluate where they are, measure how they're doing and evaluate where they want to go.

Privacy by design brings privacy-enhancing technologies and strategic partnerships to the fore. City and community leaders can build trust and earn credibility by working together across public-private partnerships to build systems that are auditable by external researchers. Building systems that are auditable and minimize data collection to what is needed is a powerful way to earn public trust.

3.3.2 HOW CAN CITIES AND COMMUNITIES EVALUATE AND MONITOR PRIVACY RISKS?

Potential privacy events directly affect individuals at the micro-level. The effects that individuals may face vary from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm. As such, these micro-level harms manifest at the macro-level and affect cities and communities in ways of lawsuits, loss of public trust, noncompliance costs, and reputational harms.

QUESTIONS TO CONSIDER

- Who should be involved in the assessment?
- How often are the assessments required?
- Will the assessments be made available publicly?
- Which use cases require comprehensive PIA?

- **Privacy Risk Management** – A cross-organizational set of processes that helps cities and communities understand how their systems, products, and services may create problems for individuals and how to develop effective solutions to manage such risks.
- **Privacy Risk Assessment** – A sub-process for identifying and evaluating specific privacy risks. In general, privacy risk assessments produce the information that can help cities and communities weigh the risks and benefits of data collection and processing as well as determine the appropriate response or remedy to identified risks. Performing a consistent risk assessment for privacy-facing initiatives allows the staff and community to understand the risks of the project as well as how that compares across projects. The level of detail of the risk assessment interview you use will depend on the privacy culture in place. Higher-level risk assessments are good for early privacy programs.
- **Privacy Impact Assessment (PIA)** – A tool to conduct a systematic risk assessment to address potential privacy risks. DHS provides detailed guidance on the reasons for conducting a PIA as well as guidance on how to conduct a PIA. Documenting PIAs and publishing them are a great way to show that the city or community is proactively taking measures to safeguard individual privacy.

TIP

Refer to this draft template for privacy risk assessment prepared by Future of Privacy Forum

DEFINITION

DHS describes PIA as a decision tool to identify and mitigate privacy risks.

CAUTION: PIAs ARE GREAT BUT...

While PIAs are excellent tools for evaluating privacy risks and communicating them to the public, they are also time consuming and require some level of expertise. For cities and communities that are resource constrained they should decide which technologies or data uses require a comprehensive PIA. This requires differentiating between high and low risk technologies. A risk assessment matrix that evaluates risk on the scale of impact and likelihood may come in handy technologies. may come in handy to identify high risk technologies.

3.3.3 SEVERAL CITIES AND COMMUNITIES HAVE LIMITED RESOURCES AND EXPERTISE TO INDEPENDENTLY EVALUATE TECH CAPABILITIES. HOW CAN CITIES AND CONNECTED COMMUNITIES OVERCOME THIS CHALLENGE?

- **Network Effect and Collaborations** – Cities and communities can benefit from the network effect and collaboratively undertake privacy impact assessments. This includes working with academic experts, consultants (hired as well as pro bono), forming a working group or reaching out to advocacy organizations and leveraging their expertise and experience in civic tech. Resource constrained cities should procure the experience and the expertise from outside, learn from it, institutionalize it and build it in-house over time. In addition, you may benefit from researching other jurisdictions that already have used the technology and experienced feedback on privacy risk management.

  Cities and communities who do not have the resources or expertise to run their own differential privacy algorithm or build their own systems should partner with academic institutions and independent researchers or learn from the experiences of the federal government agencies to build and test use cases.[9]

- **Stepping on the Shoulders of a Giant** – Cities and communities can benefit from the wisdom and experiences of other cities and federal agencies, both domestically and internationally. For instance, DHS publishes PIAs of various technologies. City of Helsinki, Finland has shorter versions of PIA for low-risk technologies.

- **Institutionalizing Knowledge and Decision Making** – Cities and communities can institutionalize knowledge and capacity building by investing time in proper documentation of a use case. Make sure to identify all the features of a project, its potential impacts and risks, mitigation measures and decisions regarding technology. Such practices will go a long way in ensuring consistent and confident decision making across departments. Providing training for employees will also play a big role in codifying knowledge and standardization in decision making.

DEFINITION

Imagine you have two otherwise identical databases, one with your information in it, and one without it. Differential Privacy ensures that the probability that a statistical query will produce a given result is (nearly) the same whether it's conducted on the first or second database.

QUESTIONS TO CONSIDER

- How will the team build relationships with potential stakeholders?
- Which city or federal agency use case aligns most closely with the problem at hand and the jurisdiction?

9 Differential Privacy definition adapted from Microsoft. (n.d.). Differential Privacy. Retrieved April 2021, from https://www.microsoft.com/en-us/research/publication/differential-privacy/?from=http%3A%2F%2Fresearch.microsoft.com%2Fpubs%2F64346%2Fdwork.pdf

3.4. PRIVACY RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		UNDERSTANDING PRIVACY	
1	Privacy in the Smart City – Applications, Technologies, Challenges and Solutions	Beginner – Intermediate	Learn more about privacy in the context of smart cities. The paper is a good reference guide to better understand the taxonomies of smart cities, types of privacy, attackers and data sources, and building privacy enhancing technologies.
2	A Taxonomy of Privacy	Beginner	Based on Dan Solove's work, the infographic provides a description of different harms that may arise from breach of privacy. This resource may come in handy for scenario planning or while thinking through the consequences of a potential privacy event.
3	10 Privacy Risks and 10 Privacy Enhancing Technologies to Watch in the Next Decade/ Future of Privacy Forum (FPF)	Beginner – Intermediate	This short paper provides information about top 10 privacy risks to look out for and 10 technologies to bake in privacy by design.
4	Differential Privacy Group/ Harvard University Privacy Tools Project	Intermediate – Advanced	Learn more about differential privacy and how it can be used.
5	Course and Educational Material on Differential Privacy/ Harvard University Privacy Tools Project	Intermediate – Advanced	
6	Nothing to Hide: Tools for Talking (and Listening) about Data Privacy for Integrated Data Systems/FPF	Beginner	Refer to Appendix A of the report to understand the basics of privacy (pg. 12), fair information practice principles (pg. 14) and refer to a list of privacy tools and resources (pg. 15-16).
7	Oakland Resident Data: Understanding What's Collected and Strengthening Privacy	All	This is a report prepared by graduate consultants from Berkeley Public Policy for the Privacy Advisory Commission of Oakland. The report provides details on the development and implementation of privacy principles in the Cities of Seattle and Portland. The report concludes with recommendations for the City of Oakland based on lessons learned from the experiences in Seattle and Portland.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		PRIVACY LEGISLATION	
8	Free Global Data Breach Notification Law Library/ Radar First	All	A free library that provides: (i) interactive maps to quickly identify U.S. laws pertaining to US states; (ii) incident risk assessment and data breach reporting requirements – as well as penalties for non-compliance; and (iii) details regarding proposed and recently passed legislation.
9	Security Breach Notification Law/ National Conference of State Legislatures	All	List of legislations across 50 states requiring governments to notify of privacy infringement involving personally identifiable information.
10	Comparison of Proposed U.S. Privacy Legislation/IAPP	All	Comparison of the three proposals for a comprehensive privacy legislation.
11	U.S. State Data Breach List/ IAPP	All	Several state agencies publish lists of reported data breaches in the state. Find the links to the lists here.
		PRIVACY IMPACT ASSESSMENT	
12	Privacy Impact Assessment/ Global Smart Cities Alliance	Beginner – Intermediate	A great resource to understand the fundamentals of PIA. It also provides references and links to a number of PIAs done by local, state, federal as well as international governments.
		PRIVACY PRINCIPLES	
13	U.S. Chamber Privacy Principles	All	10 privacy principles by U.S. Chamber to ensure consumers benefit from responsible use of data.
14	Internet Association Privacy Principles	All	Six principles and policy considerations by the Internet Association to modernize national privacy legislation.
15	The GDPR Principles	All	Read and understand the six GDPR principles. These are primarily inspired from FIPPs.
16	Privacy Principles for Facial Recognition Technology in Commercial Applications, FPF	All	FPF introduced their seven privacy principles to address concerns around personally identifiable information (PII) collected by systems using facial recognition technology.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		OPERATIONALIZING PRIVACY PRINCIPLES	
17	The City of Seattle Privacy Program	All	Provides information about setting up a privacy program, how it will be supported, department obligations, and what the privacy review process will look like.
18	Implementation Guide: City of Oakland Privacy Principles	All	The document provides an explanation of each principle and examples of how cities can operationalize those principles across the different departments.
		MISCELLANEOUS	
19	What Cities Can Learn from the Nation's Only Privacy Commission	All	Lessons learned from Oakland's Privacy Advisory Commission.
20	Best Practices Repository/FPF	All	A repository of privacy best practices and resources for smart city applications ranging from cars, drones to smart grid.
21	A Toolkit Fighting Local Surveillance/ Oakland Privacy	All	A great resource prepared by ACLU of Northern California and Oakland Privacy. This step-by-step guide provides loads of advice on coalition-building, public education, strategy, research, messaging and advocacy and samples of useful documents.

Source. Author.

“WITHOUT REFLECTION, WE GO BLINDLY ON OUR WAY, CREATING MORE UNINTENDED CONSEQUENCES, AND FAILING TO ACHIEVE ANYTHING USEFUL.”

– MARGARET J. WHEATLEY
AUTHOR OF LEADERSHIP AND THE NEW SCIENCE

SECTION 4

COMMUNITY ENGAGEMENT

4. COMMUNITY ENGAGEMENT OVERVIEW

"Why do we care?" about community engagement and some key concepts to get started.

Understanding Community Engagement – Section 4.1

- Level of community engagement & degree of public participation (4.1.1)
- Benefits of public engagement (4.1.2)
- Principles of community engagement (4.1.3)
- Scale trust through community engagement (4.1.4)
- Approaches to community engagement (4.1.5)

Planning & Operationalizing Community Engagement – Section 4.2

- Build organizational capacity (4.2.1)
- Required degree of engagement (4.2.2)
- Draft your own community engagement strategy (4.2.3)

Ensuring Meaningful Engagement – Section 4.3

- Engage stakeholders (4.3.1)
- Encourage wider participation (4.3.2)
- Select tools for inclusive engagement (4.3.3)
- Facilitate online engagement (4.3.4)
- Best practices for inclusive engagement (4.3.5)

Check out the resource repository at the end of the section.

4. COMMUNITY ENGAGEMENT

WHY DO WE CARE?

Cities and communities are being more efficient and smarter with data and increased adoption of smart city technologies. As such, the impact of the decisions made by cities and communities on their residents has grown dramatically. Cities and communities that engage and collaborate with representations from the communities create an environment that empowers residents and ensures equitable solutions to public problems.

In recent years, several smart city projects have faced severe public backlash in light of increased fear of government surveillance jeopardizing the trust people place in local governments.[2] Therefore, it is critical for cities and communities to engage, collaborate and empower their residents to ensure that they design people-centric and equitable solutions to public problems.

Community engagement, also referred to as civic engagement, means working to make a difference in the civic life of our communities and developing the combination of knowledge, skills, values, and motivation to make that difference. It means promoting the quality of life in a community, through both political and nonpolitical processes.[3]

Most cities undertake passive engagement where they focus only on the minimum legal requirement for engagement.[4] In this section, we provide guidance for active and sustained community engagement efforts. We discuss the following:

1. Understanding Community Engagement
2. Planning and Operationalizing Community Engagement
3. Ensuring Meaningful Community Engagement
4. Community Engagement Resource Repository for Cities and Communities

KEY DEFINITIONS:[1]

- **Community** – People who identify with a defined geographical area, e.g., a council ward, a housing development or a neighborhood. People who share a particular experience, or characteristic such as young people, faith groups, older people, people with disability, migrant groups, community organizations or sporting groups may also identify themselves as a community.
- **Dialogue** – An environment where people gather to talk and to understand each other, cultivate connection and deep learning through discussions on contentious issues.
- **Public Information/Outreach** – One-way communication from the government to the residents informing them about a public problem, issue or policy matter.
- **Public Participation** – Processes through which participants receive new information on the topic/problem at hand and through discussions and deliberations jointly decide on priorities or ideas and/or recommendation to inform decision of local officials.

1 National Environment Research Council. (n.d.). NERC Public Engagement Glossary of terms. National Environment Research Council, U.K. Retrieved April 2021, from https://nerc.ukri.org/about/whatwedo/engage/public/public-engagement-glossary/

2 Rainie, L., & Perrin, A. (2019, July 22). Key findings about Americans' declining trust in government and each other. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/07/22/key-findings-about-americans-declining-trust-in-government-and-each-other/; What's Fueling the Smart City Backlash? (2019, September 24). Knowledge@Wharton. https://knowledge.wharton.upenn.edu/article/whats-behind-backlash-smart-cities/

3 Oregon State University. (2021, April 8). What is Community Engagement? https://cel.oregonstate.edu/about/what-community-engagement

4 Institute for Local Government. (2016). Three Orientations of Local Government to Public Engagement. https://www.ca-ilg.org/sites/main/files/file-attachments/3_orientations_0.pdf?1500481344

4.1. UNDERSTANDING COMMUNITY ENGAGEMENT

4.1.1 WHAT ARE THE DIFFERENT LEVELS OF COMMUNITY ENGAGEMENT? HOW IS THE DEGREE OF PUBLIC PARTICIPATION DEFINED?[5]

The "ladder of citizen participation" is a prominent piece of work by Sherry Arnstein on citizen participation. Each step of the ladder represents a different degree of citizen participation ranging from non-participation to citizen control. Manipulation and therapy aim to dictate the citizens and have no place in a democratic society. Community engagement in a democratic society can be understood in the spectrum of level three – Informing – to level eight – Citizen Control.

The ladder bears close resemblance to the spectrum of public participation developed by International Association for Public Participation (IAP2) that ranges from Inform to Empower, with the former having the least and the latter having the most impact on decision making.

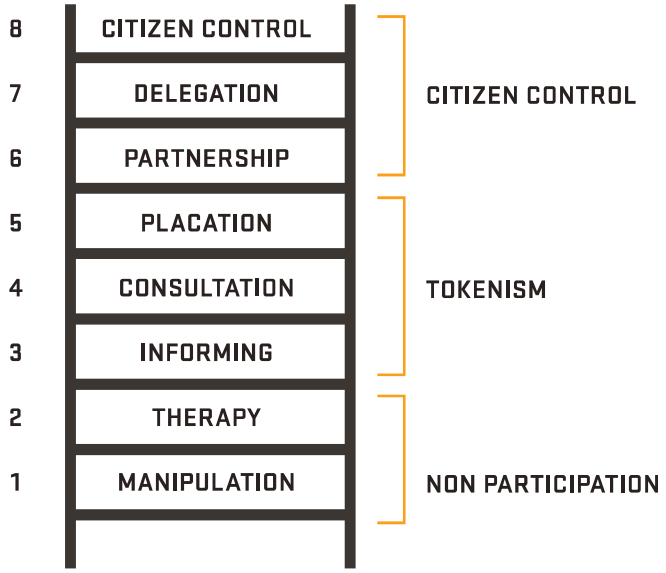
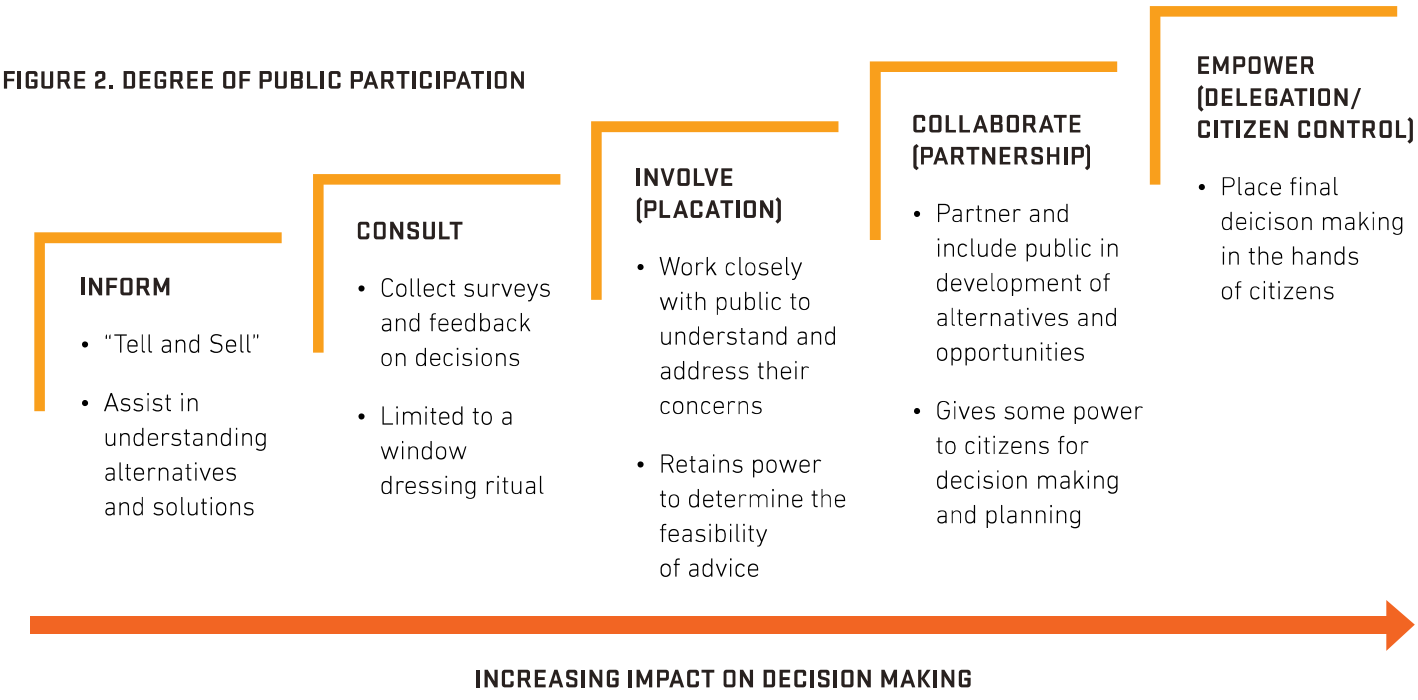


FIGURE 1: DEGREES OF CITIZEN PARTICIPATION

Source: Amstein's Ladder (1969)

FIGURE 2. DEGREE OF PUBLIC PARTICIPATION



Source: Modified based on IAP2 and Arnstein's Ladder.

5 Arnstein's Ladder of Citizen Participation. (n.d.). The Citizen's Handbook. Retrieved April 2021, from https://citizenshandbook.org/arnsteinsladder.html#collapseInnerTwo

The underlying idea behind the two concepts is that community engagement is a continuum and not a static notion. City and community leaders should decide the degree of citizen participation that is warranted based on the project/policy problem and their organizational capacity (See 2.1 to learn how to build institutional capacity for community engagement and 2.2 for deciding on the degree of participation). Cities and communities should aim to empower residents as they move up the steps from just providing a "Tell and Sell" service. This creates an opportunity for the public to co-create in the planning and decision-making process to support and reach an empowered community that makes decisions in their best interest.

TIP

Collaborating with the community to understand challenges and design solutions, and further empowering people to make decisions is a form of open policy making. The Government of United Kingdom has a comprehensive open policy making toolkit which integrates user-centric design thinking with community engagement.

4.1.2 HOW CAN CITIES AND COMMUNITIES' BENEFIT FROM PUBLIC ENGAGEMENT?[6]

"Tell me and I forget, teach me and I learn, involve me and I remember." This quote by Benjamin Franklin illustrates the importance of including residents in the community's decision-making processes. Public engagement is the essence of a democratic society and is essential for establishing transparency and public trust. Cities and communities can benefit from community engagement in the following ways: (i) better identification of resident values and needs; (ii) more informed residents; (iii) improved decision making; (iv) lower risk of public backlash at later stages of implementation; and (v) active community partnership and leadership development. These benefits further generate community buy-in and support.

4.1.3 WHAT ARE THE PRINCIPLES OF COMMUNITY ENGAGEMENT?

Well defined principles can help to establish a shared vision for engagement with different stakeholders. They are helpful indicators for planning, monitoring, and assessing the overall effectiveness of community engagement. Refer to the principles of Local Government Public Engagement by Institute for Local Government (ILG). The institute offers 10 principles for quality and effective public engagement. NIST's Guide Brief provides a set of key principles for community engagement from different agencies and organizations.

TIP

For organizing engagement around educational equity and justice refer to these principles.

6 Institute for Local Government. (2016b). What is Public Engagement? & Why Should I do it? https://www.ca-ilg.org/sites/main/files/file-attachments/ilg_what_is_public_engagement_and_why_should_i_do_it_8.31.16.pdf?1472685794

4.1.4 HOW CAN CITIES AND COMMUNITIES SCALE TRUST THROUGH COMMUNITY ENGAGEMENT?

Meaningful community engagement requires building trust among individuals and communities. Partnership building with local organizations and communities such as libraries, schools, churches, synagogues, and soup kitchens is a prerequisite for building trustworthiness. Faith-based organizations are a powerful way through which city and community leaders can build trust by proxy. This is because faith is often deeply engrained in the culture and history of a city or community, and it provides a purpose to people to come together celebrate, mourn, reflect, and help each other.[7] Refer to Faith-based Resources for Action from the Asset-Based Community Development Institute.

4.1.5 WHAT APPROACH SHOULD CITIES AND COMMUNITIES TAKE TO COMMUNITY ENGAGEMENT?

Traditional methods of community engagement focus on problems and deficiencies and see residents as victims. This is referred to as the deficit or the "vending machine" model. A problem with this approach is that it assumes a problem that has to be solved and does not include the community in the problem-solving exercise. Unlike the deficit model, the Asset-Based Community Development (ABCD), or the "barn raising" model views people as assets and focusses on engaging people to find solutions. It is important for cities and communities to "build with" the community and not for the community. Many cities and communities by default operate on the deficit model. For effective community engagement municipalities should move towards an ABCD model. To learn more about the ABCD model refer to this ABCD Talking Points Toolkit.

TIP

Read about the difference between the two models here.

7 Ives, C., & Eymeren, A. (2017, December 11). Religious faith can help people to build better cities – here's how. The Conversation. https://theconversation.com/religious-faith-can-help-people-to-build-better-cities-heres-how-88426

4.2. PLANNING AND OPERATIONALIZING COMMUNITY ENGAGEMENT

4.2.1 HOW CAN WE BUILD ORGANIZATIONAL CAPACITY FOR COMMUNITY ENGAGEMENT?

Community engagement is a massive undertaking and requires a collaborative approach for successful implementation. NIST's guide on Forming a Collaborative Planning Team and Engaging Communities provides guidance on how to build a team and who should be on the team. One lesson the guidance offers is the value of a leader for the municipality's community engagement efforts. This leader should prioritize engagement and establish a municipality's commitment to community engagement. The role can be filled by a civic leader such as a Chief Resilience Officer, a city planner or an emergency management professional. See table 1 of the NIST guide for an example of stakeholders to include on a collaborative planning team.

Cities and communities that do not have in-house expertise or capacity may also hire external consultants to assist in planning and community organizing efforts. Before engaging external public consultants read these tips for working with consultants by ILG.

TIP

- Seattle has a Community Involvement Commission that provides advice on priorities, policies, and strategies for equitable civic engagement and public participation in City decision-making processes.
- New York City has a civic engagement commission responsible for improving civic participation and improving trust.

4.2.2 HOW CAN WE DECIDE WHAT DEGREE OF PARTICIPATION/ ENGAGEMENT IS REQUIRED?

Cities and communities should decide the degree of participation (see 1.1) required based on the impact the decision(s) or the planning process has on the community.

TABLE 1. IMPACT AND DEGREE OF PARTICIPATION

IMPACT	DEGREE OF PUBLIC PARTICIPATION
High impact on whole community	Collaborate/ Empower
Hight impact on specific group/area	Involve/Collaborate
Moderate impact on whole community	Consult/Involve
Moderate impact on specific group/area	Inform/Consult

Source: Modified based on Community Engagement Toolkit for Planning.

CAUTION

The table only provides recommendations for degree of public participation based on impact. Cities and communities should decide the degree of public participation on a case-by-case basis. For instance, some projects may have moderate impact on specific groups but may still require higher degree of participation to ensure equitable outcomes.

4.2.3 HOW CAN CITIES AND COMMUNITIES DRAFT THEIR COMMUNITY ENGAGEMENT STRATEGY/PLAN?

You may be tempted to jump right to thinking about tools (see 3.3) for community engagement. However, it is important to first think about the "Why", "Who", "How" and the "What" of the community engagement process. Successful city and community leaders draft community engagement plans and strategize with the following questions in mind: (i) Why community engagement is needed (purpose); (ii) Who should be included (identify stakeholders); (iii) How will we undertake the engagement (implementation, messaging, approaches); and (iv) What we aim to achieve out of the engagement (outcomes, goals). A good example to refer to is West Seattle and Ballard line extensions community engagement guide/plan. You may wish to refer to the following frameworks to draft your own community engagement strategy:

- Five steps for creating a community engagement strategy by Metropolitan Area Planning Council.
- Strategic engagement planning by Future for Privacy Forum geared toward engagement for integrated data systems targeted more towards data privacy.
- Inclusive public engagement plan from Seattle, albeit old (2011), provides steps to design a plan, a list of questions that should be addressed and a checklist.

QUESTIONS TO CONSIDER

- What is the purpose of this engagement?
- What are the intended goals?
- What tools will be used?
- Who should be included in drafting the plan/strategy?

TIP

- Key questions for local government officials to consider while planning community engagement.
- For Community engagement around open data refer to Tactical Data Engagement and Community Engagement Impact Framework.

4.3. ENSURING MEANINGFUL COMMUNITY ENGAGEMENT

4.3.1 HOW CAN CITIES AND COMMUNITIES ENGAGE THE RIGHT STAKEHOLDERS FOR THE COMMUNITY ENGAGEMENT EFFORTS?

"If you are not at the table, you're on the menu." This anonymous quote highlights the importance of representation. It is critical to carefully engage the right stakeholders and ensure that you have a diverse table of representatives from different sections of the community. The stakeholders will differ based on the project or problem at hand. Some of the hands-on toolkits that can help with stakeholder engagement are:

- Stakeholder understanding checklist by Department of Infrastructure, Local Government and Planning, Queensland Government, Australia – Provides steps and a checklist to engage stakeholders based on their ability to influence outcomes.
- Understanding the playing field by Digital.gov – Provides a checklist, case studies and resources for understanding stakeholder groups.

QUESTIONS TO CONSIDER

- Who is not included?
- Who will be impacted directly?
- Who will be impacted indirectly?
- How can be verify that all stakeholders have been accounted for?
- Does any particular group or stakeholder have unfair or too much influence/power over the outcome(s)?

4.3.2 WHAT DIFFERENT TYPES OF PEOPLE SHOULD CITIES AND COMMUNITIES ENGAGE AND WHAT CAN BE DONE TO ENCOURAGE WIDE PARTICIPATION?

Each individual is unique. However, the way individuals interact with the municipality and their surroundings may present a pattern that may be common across different people. The table below presents the different types of people local governments interact with as they engage with the community. The list is just a subset of the variety of people one may find in a community.

TABLE 2: TYPES OF RESIDENTS

RESIDENT TYPE	DESCRIPTION
The Advocates	People who are passionate and really want to bring about a positive change in the community. These may be people at non-profits, activists, or even just ordinary residents.
The Non-Believers	People who lack civic sense, who believe that what they do doesn't matter and they can't change or influence anything.
The Unaware	People who lack the realization about if they count or that they can make an impact for instance, immigrants who have come from countries with authoritarian regimes.
The Occupied	People who are very well to do, have a busy life but do not have the time to engage in anything outside of work.

Source: Modified based on Citizen Handbook.

Community engagement is a two-way street. The onus to engage lies on both the municipalities and residents, but more so on municipalities. In some cases where there is a history of mistrust in government, city and community leaders should use extra effort to engage residents. It is important that the community engagement efforts speak to the broader community and nudge people to participate and become more involved. Use different strategies to engage the different types of people listed in the table. Refer to best practices recommended by ILG to engage the broader community.

Cities and communities should make sure that people are encouraged to participate and have accommodation that facilitates equal access and participation in the community engagement efforts. The U.S. Public Participation Playbook provides guidance on how to design participation for inclusiveness and how to provide a multi-tiered path to participation.

TIP

Refer to ILG's tip on increasing access to public meetings and events for:

- People with disability
- Immigrants
- Language Access (I)
- Language Access (II)

Refer to these checklists for engaging:

- Older people
- Younger people
- People with disability
- People from culturally and linguistically diverse background
- Unhoused people

4.3.3 HOW SHOULD CITIES AND COMMUNITIES SELECT TOOLS TO USE FOR INCLUSIVE COMMUNITY ENGAGEMENT?

One of the key elements for ensuring inclusive community engagement is to be very deliberate about the choice of tools for public meetings, activities, events, and engagements. The choice of tool will depend on the: (i) degree of public participation required; (ii) type of stakeholders; and (iii) purpose and goal of engagement (project specific, problem specific or planning). Use this toolkit to select community engagement tools based on the purpose of engagement. Refer to King County's community guide – it outlines engagement strategies/tools based on the degree and characteristics of engagement.

4.3.4 HOW CAN ONLINE ENGAGEMENT FACILITATE BROADER AND INCLUSIVE COMMUNITY ENGAGEMENT?

Online engagement helps to reach the masses thus, allowing cities and communities to make a cost-effective and positive impact at scale. A number of local governments use their websites and social media handles to engage and communicate with residents. See this good example of online engagement from Engage Arlington – a project designed to engage residents of Arlington County, Virginia, with different community engagement efforts and initiatives. Cities and communities should actively plan and invest in their online engagement efforts. Refer to this guide by Institute for Local Government (ILG) to plan your online engagement strategies and this brief for examples on using online engagement tools.

TIP

- Read these 10 tips for improving online meetings and learn more about virtual engagement tools here.
- Check out some creative and trending ideas for engagement here.

4.3.5 WHAT ARE THE BEST PRACTICES FOR ENSURING AN INCLUSIVE COMMUNITY ENGAGEMENT?

- **Be Clear About Goals and Outcomes** – The very first step to effective community engagement is clearly outlining and documenting the expected achievable goal. This also includes clearly defining the responsibilities of the community engagement team and the resident as well as the potential impact the residents will have on the final decision. For guidance on goal setting, refer to this module by U.S. Environmental Protection Agency.
- **Expand Community Connections** – Find champions within the society who can actively participate as well as encourage others to get involved. Public institutions such as public libraries, schools and colleges, and faith-based organizations can play a crucial role in spreading awareness and engaging people. Refer to this guide by the Metropolitan Area Planning Council for examples on how to connect with certain groups and brief by Institute for Local Governments (ILG) on expanding community connections.

- **Strategic Communications** – The success of community engagement banks heavily on messaging and communications. Therefore, it is important to ensure clear and transparent communications throughout the community engagement process. Refer to ILG's brief on strategic communications before, during and after beginning a community engagement effort.
- **Be Prepared to Deal with Emotional Behavior** – City and community officials often find themselves in a situation where they have to calmly deal with a disgruntled resident during community meetings and events. It is, therefore, important for officials to be trained in dealing with and diffusing such situations. Refer to this guide on how to respond to negative, emotional, or challenging comments and dealing with disruptive behavior.
- **Follow-up** – Ensure that all questions and concerns that were raised during the engagement are answered. Prepare and publish a summary of your engagement efforts as well as share the findings and next steps. At Array of Things, (Chicago) undertook massive community engagement efforts. Refer to this report summarizing their community engagement efforts.
- **Improve your Web Transparency** – Most people get information from the city or communities' website or their social media platforms/accounts. Cities and communities should design their web presence to promote transparency and ensure all the information is easily accessible with minimum clicking. Refer to this guidance on improving web transparency and refer to the resource repository for resources on improving your website.

TIP

Checklist, case studies and resources for transparently reporting outcomes and performance of participation.

- **Evaluate Success and Effectiveness** – Engaging the community is necessary but not sufficient. Cities and communities should process the gathered information and use it to achieve the desired outcomes. To this end, measuring the success and effectiveness of the community engagement efforts evaluates what worked well and what can be improved in subsequent iterations. Refer to this brief by ILG on measuring the success of public engagement, and use this rapid review worksheet to assess the effectiveness of your engagement.
- **Accept Failures and Shortcomings** – Don't get defensive when someone points out the municipality's past (or current) failings of the municipality. Acknowledge mistakes, make a clear commitment to do better, and focus on people-centric solutions.

4.4. COMMUNITY ENGAGEMENT RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		PROJECT RELATED ENGAGEMENT	
1	A Guidebook to Community Engagement: Involving Urban and Low-Income Populations in an Environmental Planning Process	Intermediate – Advanced	The document provides principles for community engagement, challenges related to engaging low-income residents around two lakes in Flint, Michigan, and step-by-step planning to engage the residents.
		COMMUNITY ORGANIZING	
2	The Community Development Handbook – A Tool to Build Community Capacity	Beginners	A comprehensive guide to get started with community engagement. It is divided into five sections that provide guidance on: (i) understanding the basics; (ii) challenges and opportunities; (iii) process behind building community; (iv) attitudes and skills; and (v) common problems and solutions.
3	The Community Development Facilitator's Guide – A Tool to Support Community Development Handbook	Beginners	A document accompanying (2). It provides examples of workshops and exercises, sample agendas, readiness checklist, and other tools required for engaging the community.
		COMMUNITY ENGAGEMENT STRATEGY, GUIDES AND TOOLKITS	
4	Community Engagement Strategy	All	A good example of an engagement strategy. It clearly identifies responsibilities and challenges, what information is needed, who is engaged, who is not reached, how they engage, and what kind of feedback is required.
5	Community Engagement Guidelines and Toolkit	Beginners	The document starts with some the basics of community engagement and introduces a framework to come up with a data engagement strategy. The highlight of this document is it provides templates to think through each of the seven steps suggested by the framework.
6	Inclusive Outreach and Public Engagement Guide	Beginners	A comprehensive guide that includes the following: (i) race and social justice implications of community engagement; (ii) strategies for inclusive engagement; (iii) key elements for effective engagement; (iv) worksheet to develop a plan; (v) matrix for engagement to decide tools based on type of engagement; (vi) template for evaluation of engagement; and (vii) glossary of key terms.
7	Community Toolbox	All	A rich resource for a wide range of templates, examples, case studies, and best practices.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
8	Public Participation Guide	All	A comprehensive guide public participation. The guide offers a wide range of resources, case studies, and self-study modules.
9	A Guide to Community Engagement in Rural and Regional Victoria	All	A standard community guide with best practices for community engagement and an engagement checklist. It is specially written for rural communities.
10	Community Engagement Toolkit	All	This is a unique toolkit as it offers a handful of templates to think through the various aspects on planning and implementing community engagement efforts.
11	Elevated Chicago Community Engagement Principles and Recommendations	All	The document provides eight principles and recommendations for improving community engagement.
12	Stakeholder Mapping Worksheet/ Future of Privacy Forum	All	This two-page worksheet provides the steps, tips and questions to consider in order to identify stakeholders. The worksheet is designed for community engagement for integrated data systems but can be tailored for other use cases.
13	Five Lessons for Tech-Powered Civic Engagement: The Charles Benton Next Generation Engagement Award Playbook	Intermediate – Advanced	The playbook features best practices in civic engagement and digital inclusion. It provides five lessons for community leaders who want to leverage increased access and next-generation technology to scale community engagement initiatives.
MISCELLANEOUS			
14	Style Guides by Government Agencies	All	A repository of style guides used by different U.S. government agencies to communicate with public.
15	Artificial Intelligence (AI): Real Public Engagement	Advanced	A guide to engagement citizen to ensure ethical use of AI.
16	Engage Victoria	All	A list of resources including community engagement framework, strategy, and templates.
17	Racial Equity Tools Community Engagement	All	A rich resource for key sites for community organizing, best practices, and tools.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
18	Connecting People to Climate Risks	Intermediate – Advanced	A comprehensive toolkit that offers case studies by team and a list of tools to engage the community.
19	International Association for Public Participation (IAP2) Values and Code of Ethics	All	IAP2 provides seven core values for the practice of public participation and code of ethics that serve as principles to ensure the integrity of the process.
20	TIERSSM framework	All	The TIERS Public Engagement Learning Lab is an interactive, results-oriented 6-month program led by ILG that provides participants in California local government with hands-on instructions, exclusive TIERS public engagement tools, individualized support of your public engagement project, follow up private consulting, and peer-to-peer learning.

“EQUITY IS THE TRUTH IN ACTION.”

– JOSEPH JOUBERT
FRENCH MORALIST AND ESSAYIST

SECTION 5

EQUITY

5. EQUITY OVERVIEW

"Why do we care?" about equity and some key concepts to get started.

Understanding Equity – Section 5.1

- Equity vs. Equality vs. Justice (5.1.1)
- Important concepts in equity (5.1.2)
- Benefits of investing in equity-focused initiatives (5.1.3)
- First steps towards equity (5.1.4)

Operationalizing Equity – Section 5.2

- Embed equity in your operations (5.2.1)
- Align data & technology programs with your equity goals (5.2.2)
- Best practices to follow (5.2.3)

Check out the resource repository at the end of the section.

5. EQUITY

WHY DO WE CARE?

From the abolition of slavery, to the Fifteenth and Nineteenth Amendments giving people of color and women the right to vote, to the Fair Housing Act, we have seen several momentous milestones in the American history. These legislative milestones marked the end of discrimination on the basis of race and other classes. The reality, however, is that even though we no longer have "explicit" discriminatory laws we still have systems, policies, and attitudes that discriminate against the historically disadvantaged groups in our cities and communities.[2]

The pandemic has disproportionately affected people of color, revealing the gruesome outcome of deeply rooted discrimination and racism in American society. To advance equity, cities and communities should first recognize the existence of inequities. City and community leaders can work together to decide how they move forward or live with the disbelief that inequities don't exist.

Equity is the key to sustainable and resilient growth in cities and communities as it creates a level-playing field for all. Prioritizing equity can help city and community leaders lay the foundations of a harmonious society where people from all walks of life can co-exist peacefully.

Efforts and resources that fight racism and improve equity should take center stage as cities and communities adopt smart city applications and use data to inform decisions that impact the lives of residents and visitors. Failure to do so will only sustain and perpetuate the vicious cycle of institutional and structural inequities that disproportionately victimize people that have historically faced discrimination in the society.

KEY DEFINITIONS:[1]

- **Affirmative Action** – Policies and practices that favor people from a certain social group who have been discriminated against historically.
- **Racism** – Racism is a doctrine or teaching, without scientific support, that does three things. First, it claims to find racial differences in things like character and intelligence. Second, racism asserts the superiority of one race over another or others. Finally, it seeks to maintain that dominance through a complex system of beliefs, behaviors, use of language and policies.
- **Segregated** – The separation or isolation of a race, class, or ethnic group by enforced or voluntary residence in a restricted area, by barriers to social intercourse, by separate educational facilities, or by other discriminatory means. The separation for special treatment or observation of individuals or items from a larger group.
- **Disadvantaged Group** – Individuals that are at a higher risk of poverty, discrimination, and violence relative to general population. This group may include but is not limited to ethnic minorities, people with disabilities, people of color, and isolated elderly and children.

1 National League of Cities. (2017, October). Municipal Action Guide Advancing Racial Equity in Your City. https://www.nlc.org/wp-content/uploads/2017/10/NLC-MAG-on-Racial-Equity.pdf; Minnesota Education Equity Partnership. (n.d.). Race Equity Glossary. Retrieved April 2021, from https://mneep.org/word/#post-4327; City for All Women Initiative (CAWI). (2015, June). Advancing Equity and Inclusion A Guide for Municipalities. https://www.cawi-ivtf.org/sites/default/files/publications/advancing-equity-inclusion-web_0.pdf; Gender Equality. (n.d.). Glossary & Thesaurus. Retrieved April 2021, from https://eige.europa.eu/thesaurus/terms/1083

2 Clark, B. E. (2018, May). Planning with An Equity Lens: Making Cities More Fair Share. National Association of Realtors. https://www.nar.realtor/on-common-ground/planning-with-an-equity-lens-making-cities-more-fair

For better or worse, much of the equity dialogue in America has been focused on racial equity as race has been the most reliable predictor of quality of life.[3] In this section, we capture equity as it relates to race, socio-economic status, gender expression, disability, age, religion, national origin, and minority groups. Equity is the fair and respectful treatment of all individuals so that their quality of life is not determined by who they were born as, who they are or who they identify as. This section provides guidance to cities and communities on how they can understand and embed equity in their operations. We discuss the following:

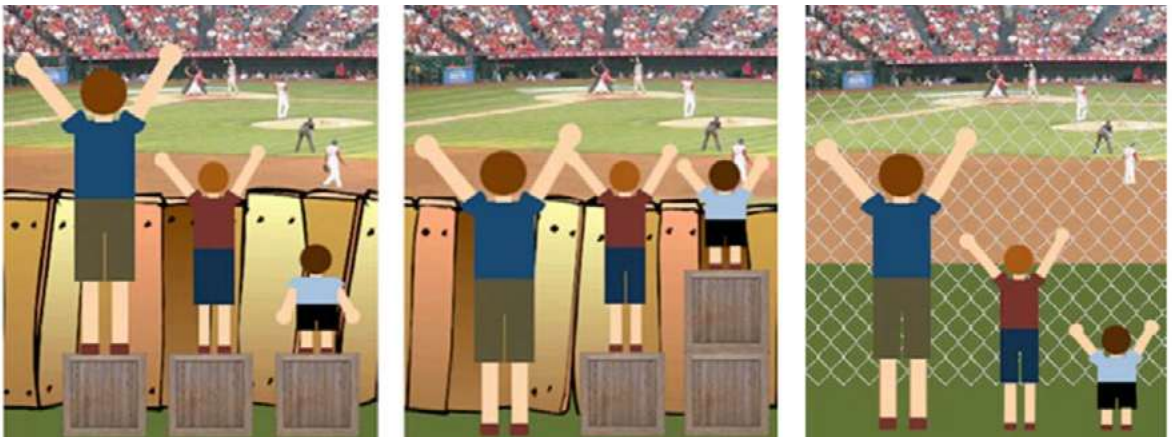
1. Understanding Equity
2. Operationalizing Equity
3. Equity Resource Repository for Cities and Connected Communities

5.1. UNDERSTANDING EQUITY

5.1.1 HOW SHOULD CITIES AND COMMUNITIES THINK ABOUT EQUITY AND HOW IS IT DIFFERENT FROM EQUALITY AND JUSTICE?

Equity, equality, and justice overlap and intersect with one another. As such, these concepts are often misconceived and even confused in our conversations about how an ideal city or community should look. One of the ways to understand the difference between the three is through the figure below.

FIG.1: UNDERSTANDING THE DIFFERENCE BETWEEN EQUITY, EQUALITY, AND JUSTICE



Source: Advancing Equity and Inclusion: A Guide for Municipalities, by City for All Women Initiative (CAWI), Ottawa
Note: This is just one version of the visual. There are a variety of visuals used to talk about the concept of Equity, Inclusion and Diversity.

3 Gee, G. C., Walsemann, K. M., & Brondolo, E. (2012). A Life Course Perspective on How Racism May Be Related to Health Inequities. Am J Public Health, 102(5), 967–974. https://doi.org/10.2105/AJPH.2012.300666

The image on the left demonstrates the concept of equality as we see the three individuals standing on same sized boxes. Equality often equates to sameness, i.e., providing everyone, irrespective of their needs and identities (see 1.2), the exact same resources. However, equality does not guarantee fairness. The center image illustrates equity where the boxes are distributed based on needs to ensure that all three individuals have a clear view (equal access) of the game. Finally, the third image illustrates justice. The fence eliminated the barrier for the individuals and addressed equal access as the root cause of the inequity (systematic barrier).

The illustration is just one example of many commonly used by researchers, activists, and non-profit organizations to explain the difference between the three concepts.

TIP

Want to understand equity and equality better? Do this exercise with your team.

5.1.2 WHAT ARE SOME OF THE KEY CONCEPTS THAT CITIES AND CONNECTED COMMUNITIES SHOULD KNOW TO BETTER UNDERSTAND EQUITY?[4]

- **Identity** – A dynamic and complex concept. To say that we are all human beings is true, but it disregards our lived experiences. By acknowledging that we all have different lived experiences, we allow ourselves to be more tolerant and open to understanding and learning from other people's experiences based on their sex/gender, ethnicity, race, national origin, disability, beliefs, economic status, age, etc. Learn more about the definition of different identities here.
- **Power** – The capacity to exercise control over or decide what's best for others, who will have access or will be denied access to a resource.
- **Privilege** – The experience of freedoms, rights, benefits, advantages, access and/or opportunities afforded to members of a dominant group in a society.[5] A privileged person is someone from a dominant/privileged group that has more power as compared to a marginalized, oppressed or disadvantaged group. Privilege is fluid and can change depending on where one is in their life. Learn more about power and privilege here.
- **Intersectionality** – A concept coined by Kimberlé Crenshaw is based on the recognition that individuals can have multiple identities that intersect with one another. Intersectionality refers to the interplay of one's identities, the status of those identities, and the situational context of how, when, and where those identities show up and influence personal experience(s) within multiple dimensions of societal oppression.[6] Learn more about intersectionality here and also refer to Section 2.1 to learn why municipalities should apply the intersectionality lens.

Enhancing equity requires changing power structures that sustain racism and discrimination. Therefore, understanding the different identities, their intersection, and the existing power structures within different social groups can help city and community leaders achieve greater equity.

TIP

A more comprehensive list of terms that cities and communities should understand can be found here and on pg. 17-18 of this guide for municipalities. For Racial Equity concepts refer to this resource.

4 University of Colorado Denver. (n.d.). Power & Privilege. Retrieved April 2021, from https://www1.ucdenver.edu/offices/equity/education-training/self-guided-learning/diversity-equity-and-inclusion-101#PowerPrivilege

5 City of Ottawa and City for All Women Initiative. (2015). Equity and Inclusion Lens Handbook. City of Ottawa and CAWI. https://www.cawi-ivtf.org/sites/default/files/publications/ei-lens-handbook-en-web-2018.pdf

6 University of Colorado, Denver. (n.d.). Office of Equity - Intersectionality. Retrieved April 2021, from https://www1.ucdenver.edu/offices/equity/education-training/self-guided-learning/intersectionality

5.1.3 WHAT ARE THE BENEFITS OF INVESTING IN EQUITY-FOCUSED INITIATIVES?

Smart city applications create opportunities for cities and communities by connecting their neighborhoods and helping them make informed data-based decisions to deliver goods and services efficiently. The flip side of these opportunities is that they can threaten a city or community's overall health if the benefits from use of technology is inequitably shared among the member of the community.[7] Therefore, city and community leaders should invest in equity-focused initiatives to ensure that the benefits of smart city applications lead to sustainable and equitable outcomes.

Equity is a resiliency challenge. Inequities inhibit long-term growth and prosperity are a chronic stress on the city's health. Investments in equity-focused initiatives may not bear fruits immediately but they can preserve and protect a city or community's true culture and identity in the long run. Equity is a driver for sustainable development that can unlock resources to generate higher efficiency in the long run.

5.1.4 HOW CAN CITIES AND COMMUNITIES GET STARTED WITH EQUITY?

- **Look Inward Before Looking Outward:** Start by tasking your Human Resource (HR) department to undertake an assessment of equity and diversity at your workplace. A diverse workplace is essential to ensure representation of the community that you serve or want to attract. Greater representation translates to a range of insights and perspectives that the municipality can leverage on to define its equity goals. Identify group(s) that are un- or under-represented and take immediate steps to build a more diverse and inclusive workforce. To ensure equity in hiring, the city of Portland has an Equal Employment Opportunity Affirmative Action Plan for Minorities & Women. Asheville has a public facing workforce equity dashboard that represents its commitment to ensuring equitable hiring and promotion outcomes within the city.

  It is important to understand that diversity and inclusion without equity is not sustainable. Promoting a diverse

QUESTIONS TO CONSIDER

- What proportion of the workforce are people of color/women/from LGBTQ+ community/have disabilities?
- How diverse is higher level management?
- What affirmative actions can be taken to ensure diversity in hiring and promotions?

DEFINITION

Diversity refers to differences in the values, attitudes, cultural perspective, beliefs, ethnic background, sexual orientation, gender identity, skills, knowledge and life experiences of each individual in any group of people.

7 Greene, S., Macdonald, G., & Arena, O. (2019). Technology and Equity in Cities. The Urban Institute. https://www.urban.org/sites/default/files/publication/101360/technology_and_equity_in_cities_1.pdf

workplace is the first step towards equity but not an end in itself.

- **Build Your Equity and Inclusion Team**: Assign resources and budget to build an equity and inclusion team. This team will be responsible for assessing gaps, operationalizing equity, meaningful community engagement, understanding the historical context, and forging strategic partnerships to advance equity goals in the municipality. Several cities have appointed a Chief Equity Officer to oversee their equity and inclusion initiatives. Cities and communities that are resource constraint should consider hiring at least an equity manager to establish their commitment towards equity.

- **Accept and Acknowledge:** One of the major challenges to equity in cities and communities is the disbelief that inequity exists. The first step to solving a problem is acceptance and acknowledgement of the problem. Review and understand the historical context, collect data and document inequities in your city and community. Several cities have created and published equity maps. Some examples include Equity Atlas by the city of San Antonio and Racial Equity Mapping by the city of Ashville. Other organizations that map equity are Community Information Now, National Equity Atlas (also a great resource for equity indicators), and the Demographic Statistical Atlas.

- **Make a Clear Commitment to Enhance Equity:** Cities and connected communities should make a clear and explicit commitment to equity. This can be in the form of a public declaration by: (i) creating an Office of Equity or an Equity Initiative; (ii) releasing a statement to advance equity goals (see the city of St. Louis Park); (iii) defining equity and adopting equity as a guiding principle for the operations of the city or community (see the city of Tacoma); and/or (iv) providing resources and support to historically disadvantaged communities (see the city of Asheville mini-grants for racial healing and the city of Austin's Mini-Grant Fund for grassroot community organizations). Make sure

TIP

Refer to suggested steps for building your team on pg. 11 of this guide by the National League of Cities.

TIP

Use the Urban Institute's Spatial Equity Data Tool to map inequities in your city.

QUESTIONS TO CONSIDER

- What indicators should be collected to measure inequities? (See National Equity Atlas or the City of Tacoma's Equity Index)
- How can we source data on equities?
- What's the best way to share this data both within and outside the organization?

that this commitment is not just limited to lip service or window dressing (see Section 2 on Operationalizing Equity).

- **Benchmark Where You Stand:** Identify your baseline by assessing where you stand. An assessment of practices and the status quo across different departments can help to determine the gaps and identify the areas for improvement. Such an assessment will also help establish equity goals for the municipality. You may refer to the "Environment Scan Checklist" in the Advancing Equity and Inclusion guide (pg. 33 to 36) modify it to suits your organization. Use the activity to identify gaps and obstacles and come up with strategies to overcome them (see Advancing Equity and Inclusion guide). Alternatively, you can also undertake the Racial Equity and Justice Initiative (REJI) Organizational Assessment to assess where you stand.

In the next section, we focus on how cities and communities can operationalize equity and align it with organizational goals and outcomes.

TIP

If you can only do three things you should:

- Research, understand and document the historical context and inequities in your city and community.
- Assess diversity and representation at workplace.
- Commit for the long haul. Start with small steps to advance equity at workplace and in your community.

5.2. OPERATIONALIZING EQUITY

5.2.1 HOW CAN CITIES AND COMMUNITIES EMBED EQUITY IN THEIR OPERATIONS?

- **Set Equity Goals and Develop an Action Plan**: The most crucial step to operationalizing equity is to document equity goals and outline actions that should be undertaken to achieve those goals. While these goals and strategies will be unique for each municipality there are several good examples to look at such as the city of Asheville's Equity Action Plan, San Francisco's Racial and Social Equity Action Plan and 19 actions identified by Portland's Equity Initiative. Use GARE's Racial Equity Action Plan – A How-to Manual to draft your own equity goals and action plan.
- **Apply an Intersectionality Lens:** Cities and connected communities can take a step towards understanding equity by identifying the different lived experience of

TIP

- Read Section 6 of this guide for steps to create a racial equity plan.
- Encourage your team to conduct the "Intersectionality Wheel Diagram" activity from the Advancing Equity and Inclusion guide.
- Read more on how to put intersectionality into practice.

their residents. The very first step to adopting the lens of intersectionality is by asking your employees to understand their own identities. Adopting the intersectionality lens can help cities move beyond groupthink and consider how different identities interact with the municipality.

- **Educate and Train:** Invest time and resources to educate your employees and encourage them to engage in discussions about equity or partner with other cities, communities, or non-profits to bring in speakers and conduct workshops to raise awareness about equity within the organization. The city of Austin, Texas, conducted "Undoing Racism" in partnership with the People's Institute for Survival and Beyond to train over 500 community members since 2007. Refer to resource repository for resources on training and education.

  Cities and communities can also learn a great deal by engaging with communities. Refer to the Community Engagement section of this guide to learn more.

- **Take an Equity Approach to Budget –** To ensure equity is at the forefront of decision-making across all departments make it a priority and a guiding principle for how the municipality allocates budget. The city of Asheville created an Equity Budget Tool to include equity considerations into their policies and practices for department budgets. The city of Seattle has been using a Racial Equity Toolkit to assess policies, programs and budget issues since 2012. Other cities such as Austin and Philadelphia have also taken steps to integrate equity into their budget-making process.

- **Equitable Procurement and Contracting** – Cities and communities spend millions of dollars on the procurement of various goods and services to serve their municipalities. Equity in procurement and contracting can be a powerful recovery tool that supports and empower businesses owned by people from disadvantaged communities. Read about the innovative tactics that cities are using to enhance equity and learn about five cities that are setting an example of equitable procurement.

TIP

Read GARE's recommendations on best practices for local governments to advance equity in procurement.

5.2.2 HOW CAN CITIES AND COMMUNITIES ALIGN DATA AND TECHNOLOGY PROGRAMS WITH EQUITY GOALS?

Data-driven decision-making has helped cities and communities distribute their resources more efficiently. If used responsibly, data can also help to address inequities and make them more visible. Cities and communities should actively take steps to ensure that data sharing and use remains equitable and transparent and does not lead to perpetuation of organizational and structural inequities. Actionable Intelligence for Social Policy (AISP)'s comprehensive toolkit provides guidance on

TIP

Refer to the list of questions in the AISP toolkit to think though for integrating equity into the data life cycle.

how cities and communities can centralize racial equity in their data integration and sharing practices. To assimilate equity more broadly into technology programs, refer to the guide by the Urban Institute for Creating Equitable Technology Programs. The guide provides several examples and case studies of cities that have embedded equity in their technology programs.

5.2.3 WHAT ARE THE BEST PRACTICES FOR CREATING EQUITABLE CITIES AND COMMUNITIES?

- **Train, Educate, Empower, Repeat** – Enhancing equity is a long iterative process and requires continuous learning and training. This includes not only training and educating staff members but also community members and residents. The city of Boston, Massachusetts, runs a series of monthly community race dialogues and has trained facilitators and engaged thousands of residents over the years.
- **Assess and Track Progress** – Take stock of your impact and track your progress. Identify improvements as well as shortcomings. This assessment should guide goal setting for subsequent versions of an action plan. Austin, Texas, has its own Equity Assessment Tool (pg. 10) that it uses to assess the performance of its departments towards advancing their racial equity goals. The Racial Equity Index can help you assess how your city or community is doing as compared to others. The tool can also be used to identify gaps and set equity goals. The next step will be to get the assessment reviewed by an independent third party to establish credibility and trust.
- **Sustain Impact**[8] – Any work around equity will receive pushback from all levels because it challenges the status quo and those in privileged and powerful positions. Therefore, it is important to build momentum and bring about organizational changes to promote equity. Identify champions across all departments who can advocate and enforce guidelines and practices for promoting equity. These champions can play an instrumental role in developing shared practices across departments, mentoring staff as well as countering any resistance to efforts for advancing equity. Get support from all levels, ensure a clear messaging and commitment to equity at all levels of management.

TIP

Start small! Refer to this guide to develop indicators to measure your performance and assess your progress.

DEFINITION

A champion is a person who assumes leadership by working with others to create and influence change in the wider community.

TIP

Refer to this toolkit for Community Agreements for Productive Conversations on Race. Use this template to negotiate tangible community benefits for public and private investment.

8 City for All Women Initiative (CAWI). (2015, June). Advancing Equity and Inclusion A Guide for Municipalities. https://www.cawi-ivtf.org/sites/default/files/publications/advancing-equity-inclusion-web_0.pdf

- **Engage the Community and Build Relationships** – The most important seats at the table for equity conversations should be reserved for the members of the community. Work with representative organizations and residents and build accountable relationships to ensure inclusive and equitable growth in your municipality. For example, a Community Benefits Agreement (CBA) can serve as an effective tool for ensuring equitable outcomes in development projects.

- **Follow Through and Follow Up** – Communicate your progress and demonstrate results with the community to keep everyone on the same page. Publish internal assessments to establish transparency – see Asheville's internal audit report on Equity and Inclusion Assessment. Report the assessment findings to community members especially to those who actively participated in the meetings. Create channels for community members to submit queries and questions regarding the assessment. Publish frequently asked questions or concerns on your website.

- **Collaborate and Learn from Others** – Partner and collaborate with other cities and communities that may share similar historical contexts or inequities. For cities and communities that are resource-constrained, this may be the most feasible and cost-effective approach to enhancing equity. Additionally, learn from the others who are further along in their journey to integrating equity in their organizational outcomes and goals. For example: (i) Austin's Equity Action Team has evolved over time into a community body that provides learning and networking opportunities to those interested in equity. The group also includes cities from outside Texas; and (ii) Racial Equity Here was a partnership of five cities – Albuquerque, Austin, Grand Rapids, Louisville, and Philadelphia – to improve equity. Learn about their experience of operationalizing racial equity.

QUESTIONS TO CONSIDER

- With whom can we partner to conduct training?
- What indicators should be used to track progress?
- How can we verify the validity of these indicators?
- How can we communicate the finding and progress so that it reaches all representatives of the community?
- Which local organizations can help advance equity goals?
- How can we forge strategic partnerships with other cities and communities?

5.3. EQUITY RESOURCE REPOSITORY FOR CITIES AND COMMUNITIES

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
		GUIDES	
1	Improving Procurement Processes to Promote Economic Equity	All	The document provides several case studies and an implementation plan for advancing economic equity through procurement.
2	Equitable Contracting and Procurement	Beginner	The resource explains equitable contracting and procurement, identifies resources to implement, shares key considerations and provides examples of where it is working.
3	Advancing Racial Equity and Transforming Government	Beginner – Intermediate	A comprehensive guide that discusses six best practices to advance racial equity. The discussion is augmented with case studies from eight cities.
4	Racial Equity Impact Assessment Guide	Beginner	The two-page document explains what a racial equity impact assessment is, why it is needed and when it should be conducted. The document also provides some questions to consider in order to anticipate, assess and prevent potentially adverse consequences of proposed actions on different racial groups.
5	City for All Women Initiative Publications	All	A list of publications around promoting racial and gender equity in municipalities.
		TOOLKIT	
6	Racial Equity Tools	All	An incredible resource that provides a comprehensive list of resources and curricula for training, planning, implementing, and evaluating racial equity.
7	Racial Equity Toolkit – An Opportunity to Operationalize Equity	Beginner – Intermediate	The document explains what racial equity tools are, who should use them and how they can be used. It also offers examples and use cases to help you get started with racial equity tools.
8	Equity Assessment Tool	Intermediate – Advanced	The report uses different case studies to explain equity metrics and provides tools to assess potential strategies through the lens of equity.
9	Racial Equity Toolkit	Beginner	This easy-to-read and use toolkit from the city of Seattle can be used to assess policies, initiatives, programs, and budget issues. It offers six steps, worksheet and resources to help with assessment.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
10	Texas Equity Toolkit	Beginner – Intermediate	It's a good resource and template to develop your local equitable access plans.
11	All-In Cities Policy Toolkit	All	A great resource for policy toolkits by topic area.
12	Racial Equity Resource Guide	All	A database for resources and guides that can be used by cities and communities for trainings and advancing their racial equity efforts.
13	Portland's Bureau Racial Equity Plans	All	A collection of resources, equity plans, and training material from the city of Portland.
14	Texas Model by Joyce James	All	A model developed by Joyce James to improve equity outcomes for all children. The model was implemented by the Texas Department of Family and Protective Services.
15	Diversity Toolkit: A Guide to Discussing Identity, Power and Privilege	All	The toolkit offers several activities for groups of up to 60 people to have a discourse on issues of diversity.
ADVANCING EQUITY AT WORKPLACE			
16	The Roadmap for Racial Equity – An Imperative for Workforce Development Advocates	All	Refer to pages 22 and 25 of this report. The following pages discuss including racial equity goals in local and state government workforce development and investing in infrastructure and technical assistance to achieve equity goals.
17	Advancing Equity	All	Three short articles on: (i) Transforming Culture — An Examination of Workplace Values Through the Frame of White Dominant Culture; (ii) Addressing Bad Behavior in Your Civil Justice System; and (iii) Relearning America's History of Race — A Beginner's List of Resources
EQUITY AND RESILIENCE REPORTS			
18	Resilient Boston – An Equitable and Connected Cities	All	The report outlines various initiatives and undertaken by the city. It also outline's the city's strategies and its visions.
19	Resilient Cities at the Forefront	All	The report discusses the link between urban resilience and racial equity. The report showcases best practices using several examples of equity initiatives in cities such as Boston, Seattle, and Toronto.

NO.	TITLE/ORGANIZATION	LEVEL	WHAT CAN YOU EXPECT TO LEARN?
20	Our Equitable Future – A Roadmap for the Chicago Region	All	The documents provide the equity roadmap for the Chicago region. It provides targeted recommendations for advancing equity goals and also features examples of local progress and initiative.
21	The Future of Equity in Cities	All	A National League of Cities report discusses the importance of equity and looks at infrastructure, economic development, and public safety through the lens of equity.
22	Technology and Equity in Cities	All	A comprehensive report by the Urban Institute that talks about emerging equity challenges and opportunities for smart infrastructure, shared mobility, civic technology and technology-enhanced data analytics.
23	Institutional Racism and Systematic Inequities	All	A report from Austin, Texas that captures the background and context of historical racism and makes recommendations to improve equity in the city.