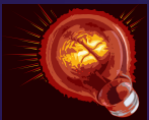


Think To DO Institute



The Value of a National Data Framework To Better Measure Country Resilience 2024

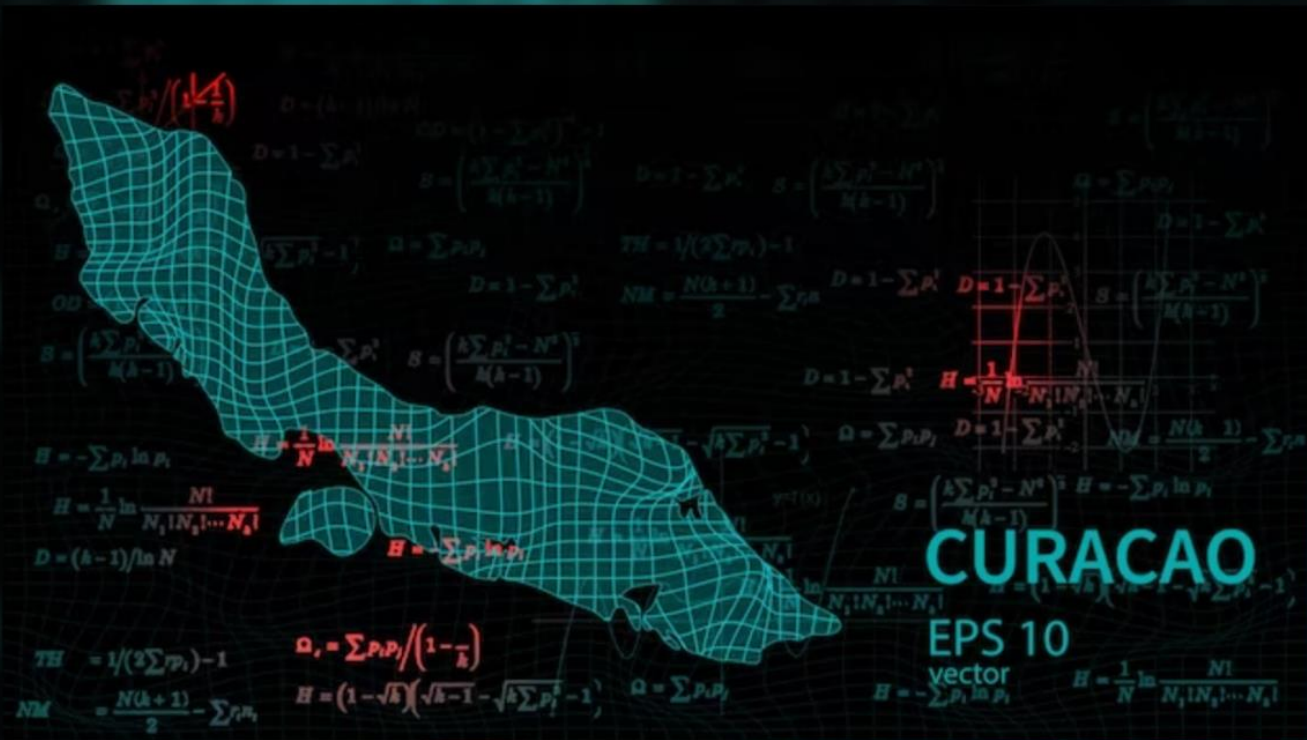


We wish to thank the many persons in the Think To DO Institute and those from various institutions who assisted in the identification of data sources, contributed expertise and who offered helpful suggestions to this research initiative.

Copyright 2024, Think to DO Institute



The Think To DO Institute is an independent, apolitical think tank located in Curaçao, Dutch Caribbean. The T2DI has as its purpose to help Curaçao become a more resilient society by producing research that is based in best practice, and which delivers practical solutions to the barriers that hold the community back from becoming more resilient. Research evidence shows that Resilient Societies are created by attention to people, to organizations, to place, and to knowledge. Resilient Societies design, redesign organizations, institutions, and systems to better absorb disruption, operate under a wide variety of conditions, and shift more fluently from one circumstance to the next. For more information about the Think To DO Institute, visit the website: www.thinktodoinstitute.com



Background and Methodology

Background

The Think To DO Institute has focused all of its research around the four areas of resilience: People, Place, Knowledge and Leadership. In designing its various research around fragile states, mindsets, and social cohesion, the Institute determined that there were not sufficient data sets available to the research process to frame challenging social and economic circumstances.

It was known that resilience assessments are important because they help to identify areas of strength and areas where improvement may be needed. Resilience assessments can also promote awareness, leading to more effective use of interventions. It was with this knowledge in hand that the institute decided to engage in deeper research into the necessary data frameworks needed to support more effective research outcomes.

The fact that the autonomous nation of Curaçao has had nine governments since its creation thirteen years ago, and the fact that the planned government central planning entity was not created at that time has contributed to the lack of data. The lack of implementation of a law that was placed on the books in 2013 to address data sharing has delayed a quality data collection sharing process.

Data collection is an essential tool for the advancement of developing countries such as Curaçao. Data provides valuable insights into the needs and priorities of the community, identifies areas of opportunity for economic growth, and tracks progress towards development goals. Sufficient information must be provided in accessible and culturally appropriate ways. Providing information about benefits and disadvantages of the results of data collection and the research projects that use the data to develop policies, processes and their outcomes allows people time to think about the issues, consider implications, and formulate their views.

Resilience research has as its foundation the goal of improving people's lives. By allowing researchers to measure and act, an effective data system can enable individuals, and public and private organizations to improve the quality of people's lives.

As a result of this think tank's research of best practices in country-wide data collection processes, it was determined that a national data framework is essential to establish data democratization and allows public and private employees all the technical skill sets and abilities to access and act on data. Further, this allows teams to accurately set goals, measure performance, strategize and innovate with confidence and autonomy. Transparency for the consumer is ensured because the data is processed, protected and shared within global norms.

The Institute uses internationally normed surveys for various research areas because these allow for documented validity and cross-country comparisons. This comprehensive social science approach, data from three main streams — pre-existing quantitative data sets, content analysis, and qualitative expert analysis — is triangulated and subjected to critical review to obtain final scores for the indexes used.

A comprehensive national data system is necessary to provide quantitative data sets, content analysis, and qualitative expert analysis.

Therefore, the determination was made to conduct the deep dive research into the best models for national data frameworks to guide resilient country development.

Methodology

The key research question was generated because of the lack of access to or the lack of local data for use by the Think To DO Institute or other entities wishing to make data-driven decision making.

After literature review and design thinking methodologies to guide inquire, the following research question was created:

What actions (administrative, legal, technical) are needed to make a national data framework implementation with access to all successful, and how can the results be measured? What makes the implementation successful?

Data maturity and data governance are two related but distinct concepts in the field of data management. Data maturity refers to the level of an organization's ability to effectively manage and utilize its data assets to drive decision-making and achieve desired outcomes. It focuses on the organization's overall capability to manage data effectively. Data governance, on the other hand, is a framework of policies, procedures, and processes that ensure the proper management of an organization's data assets. Both concepts were critical to the research's clarity.

A mixed methodology was selected in the research on Openness of Data on Curaçao in order to implement the strengths of both qualitative and quantitative research methods. This approach is beneficial because it allows each methodology to counteract the weaknesses of one or the other of the methodologies, especially because of the scope of the research question and the need to compare best practice to local conditions.

The criteria for assessing data openness were divided into two categories. First, criteria like Accessibility, Machine-readability, Structured vs Unstructured, Downloadable, Documentation, and Openness were considered more straight-forward to assess. Second, criteria like Frequency of Updates and Data Quality were considered more complex.

Quantitative Research Questions revolved around the local implementation to determine how many, how often, how knowledgeable and how satisfied local entities were with the administrative, legal and technical aspects of data sharing (data frameworks) related to *Data Governance* and *Open Data*. One instrument was a closed-ended survey. The other was a benchmarking exercise of publicly available local public and private sector data.

The *Data Governance Checklist* (adapted from US Version) was administered to a representative cross-section of the private sector with limited success.¹ The purpose of this checklist is to assist public and private sector entities with establishing and maintaining a successful data governance program to help ensure the individual privacy and confidentiality of personal data records. It measured an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data, from acquisition to use to disposal. This includes establishing decision-making authority, policies, procedures, and standards regarding data security and privacy protection, data inventories, content and records management, data quality control, data

¹ *Data Governance Checklist*, Privacy Technology Assistance Center, National Association of State Chief Information Officers, United States, 2011.

access, data security and risk management, data sharing and dissemination, as well as ongoing compliance monitoring of all the above-mentioned activities.

Specific best practice action items about the key data privacy and security components of a data governance program are summarized below. This document focuses on scope of and overview of data governance responsibilities no matter the public or private type of system of the stakeholder. It is

hoped that this checklist can assist any entity in becoming compliant with local and international data privacy policy compliance.

Qualitative Research focused on the best practices globally in the creation of national data policies and data policy frameworks. Detailed fact finding related to policies, processes, outputs, outcomes, structures, timelines and funding mechanisms were reviewed. The research was interested in the motivation, experiences, problems, data transparency, and relationships involved in the creation of such frameworks.

Major contributors to this body of research were consulted and as a result the research team completed online certification in the Nordic Institute for Interoperability Solutions(NIIS) basic training courses in understanding and designing a *national data policy framework*.²

The World Economic Forum(WEF) Data Policy framework was also consulted to review the various aspects of data policy as the WEF had compiled research from multiple member countries. The common policy areas and structures were then organized and contributed to the content of this research document.³

² *National Data Policy Framework*, Nordic Institute for Interoperability Solutions(NIIS), Tallinn, Estonia. 2022.

³ *Data Policy Framework*, World Economic Forum, Cologny, Switzerland. 2022.

Contents

Background	4
Methodology	5
1 What does it mean to develop “data maturity”	10
1.1 Results of the Think to Do Survey	12
2 Data Policy Framework as a driver of institutional policy decisions	17
2.1 What is currently in place	18
2.2 What are some concrete and actionable suggestions	18
3 Fundamental Digital Systems; The development of a modern digital system	20
3.1 Adoption of digital transformation	20
3.2 Current State of Connectivity	21
3.3 Current state of digital payment system	26
3.4 Current state of Digital identity	29
4 Data Policy Framework Elements	31
4.1 CIA Triad	31
4.2 Data confidentiality	32
4.3 Data integrity	32
4.4 Data availability	32
4.5 Data interoperability	32
4.6 DIE Triad	33
5 European Interoperability Framework (EIF)	35
5.1 Interoperability Governance	36
5.2 Integrated public service governance	36
5.3 Legal interoperability	37
5.4 Organizational interoperability	37

5.5	Semantic interoperability	38
5.6	Technical interoperability	38
5.7	Netherlands towards Interoperability	38
6	Data concepts and the Role of Open Data in National Development	40
6.1	Concepts of data and data collection	41
6.2	Grading Framework for data sources in Curaçao	48
6.3	ISO standards for data	52
6.4	Methodology of choice	55
6.5	Best practices for managing and making data publicly available	55
7	The industry practice for the use of data within mass media communication	57
7.1	Types of mass media communication	57
7.2	What are Social Media and Influencers	58
7.3	Reach, Resonance and Relevance	59
7.4	Integrity, accountability, in data from mass media	60
7.5	The effects of information and disinformation on public opinion	62
8	Ethical Boundaries and Concerns	63
8.1	Safeguarding and Guardrails	63
9	Working across international data frameworks (GDPR, CCPA, PDPA(Asia/Singapore)	65
	Conclusions and Recommendations	69
	Glossary	74
	Figures	79
	Resources	81
	Bibliography	82



National Data Policy Framework

Chapters 1-9

1 What does it mean to develop “data maturity”

Data maturity refers to an organization’s ability to effectively manage and leverage data to drive business value. To do so, organizations must develop and improve data-related capacities, processes and strategies throughout the organization. It requires systemic organizational reform. When an organization has a high level of data maturity, it exhibits specific data characteristics related to data governance, data infrastructure, data strategy, data integration, data analytics and insights, data culture and skills, and data privacy and security.

Developing data maturity is an ongoing process that requires continuous improvement and investment in data-related capabilities. At its best, it involves the collaboration of various stakeholders, including data professionals, IT teams, business units, and leadership, to foster a data-driven culture and maximize the value of data assets.

It is important to first define the scope within these data characteristics to fully understand what it means to develop “data maturity”. How this *national data policy framework* helps drive policy decisions within the public and private sector is further detailed in Chapter 2.

Data governance means that data is governed and managed effectively across the organization. There are clear policies, processes, and standards in place for data collection, storage, quality, security, and privacy.

A well-defined *data strategy* aligns the organization’s overall business goals and objectives. The strategy outlines how data will be used to drive decision-making, innovation, and competitive advantage.

When *data integration* is achieved organizational silos are minimized, and data is consolidated and made available for analysis and decision-making purposes.

Mature organization employs *data analytics and insights* to derive meaningful insights from data to uncover patterns, trends, and correlations that drive business outcomes. This includes data mining, statistical analysis, machine learning, and predictive modeling.

Having *data culture and skills* means employees understand the value of data and are equipped with the necessary skills to work with data effectively. Data literacy is encouraged, and training programs may be implemented to enhance data-related skills.

Lastly, and most importantly, the mature organization prioritizes *data privacy and security*, adhering to relevant regulations and implementing measures to protect sensitive data from unauthorized access or breaches.

It should be noted that traditional governance models may hinder the agility required to harness the full potential of data. Data maturity, when combined with agile governance practices, enables organizations to harness the power of data in a dynamic and responsive manner because it emphasized the need for iterative, collaborative, and adaptive approaches to governance that align with agile development methodologies.

Although several models exist from reputable companies such as IBM, Stanford, Gartner, and Oracle among others, there is no globally recognized standard for a *data governance maturity model*.⁴

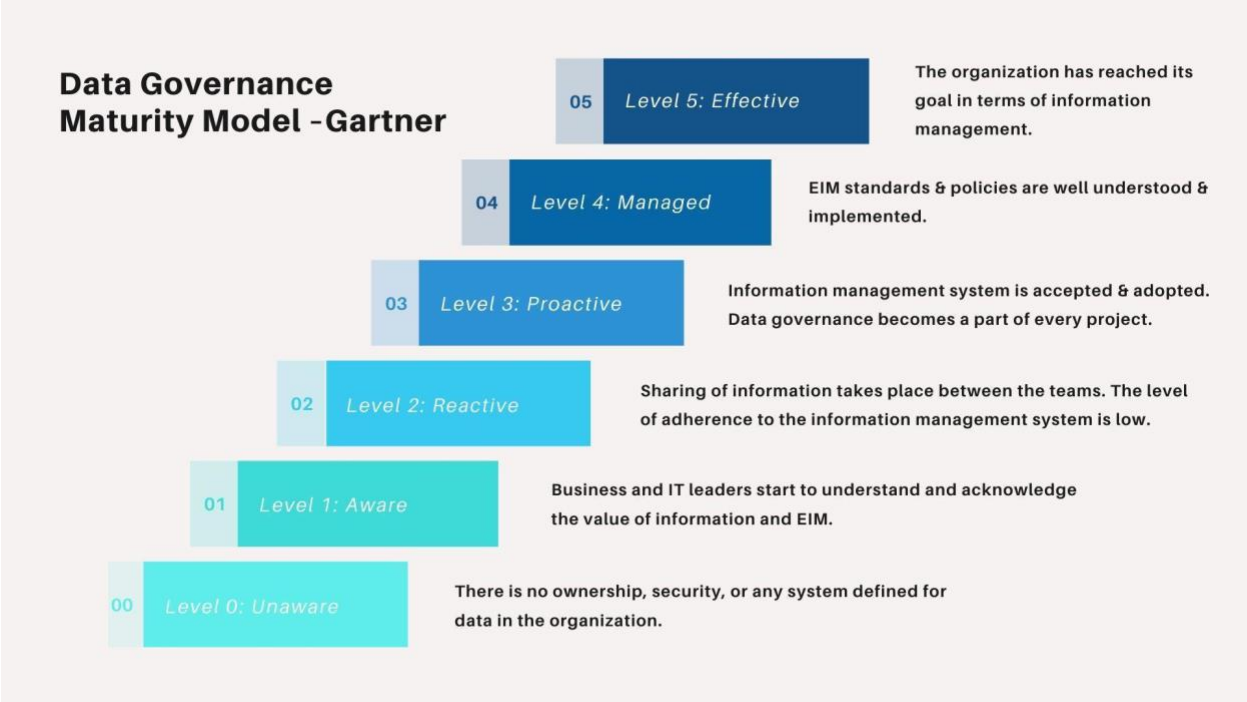


Figure 1 : Gartner Data Governance Maturity Model

Data maturity encompasses several key aspects. Data policy frameworks maturity is measured by whether the entity, whether private or public, has developed the necessary practices in each of the following areas:

- **Data Governance:** Developing robust data governance practices involves establishing clear policies, procedures, and guidelines for data management, including data quality, privacy, security, and access. It ensures that data is governed and managed consistently across the organization or country.
- **Data Infrastructure:** Building a solid data infrastructure involves setting up the necessary systems, tools, and technologies to efficiently collect, store, and manage data. This may include data warehouses, databases, data integration platforms, and data management tools.
- **Data Quality and Integration:** Focusing on data quality involves implementing measures to ensure data accuracy, completeness, and consistency. Data integration ensures that data from various sources is harmonized and combined effectively for analysis and decision-making.
- **Data interoperability:** Data interoperability, refers to the ability of different systems or components to exchange and use data seamlessly and effectively. It involves ensuring that data can be shared, understood, and utilized across different systems, platforms, or organizations without loss of meaning or functionality.
- **Data Analytics and Insights:** Advancing data maturity involves building analytical capabilities to derive meaningful insights from data. This includes employing data analysis techniques, such as statistical analysis, data mining, machine learning, and predictive modeling, to extract valuable insights and support evidence-based decision-making.

⁴ <https://www.hitechnectar.com/blogs/data-governance-maturity-models-explained/>

- **Data Culture and Skills:** Developing a data-driven culture within an organization or country involves promoting the understanding and appreciation of data, encouraging data literacy and skills development among employees, and fostering a mindset of using data to drive decision-making.
- **Data Privacy and Ethics:** Ensuring data maturity also involves addressing data privacy and ethics considerations. This includes adhering to legal and ethical standards for data handling, protecting individuals' privacy rights, and ensuring responsible data usage and sharing practices.

By advancing these aspects of data management and utilization, organizations or countries can enhance their ability to leverage data as a strategic asset, make data-informed decisions, drive innovation, and achieve their goals more effectively. Data maturity is an ongoing journey, and organizations or countries may continuously evolve and improve their data capabilities over time.

The results of the Data Maturity Survey conducted by the Think To DO Institute in early 2023 indicates that across sectors that the levels of data maturity are very low falling in the Level 1 and Level 2 of the Gartner's Data Maturity Framework.⁵ This indicates that the characteristics listed above in this Chapter must be developed through cross sector, public and private development initiatives.

1.1 Results of the Think to Do Survey

The Think To Do Institute National Data Framework sounding session survey aimed at exploring the critical dimensions of data management within organizations. In an era dominated by digital interactions and evolving privacy regulations, it is imperative for businesses to uphold certain principles to safeguard sensitive information and build trust with stakeholders.

This survey delves into key aspects of data management, focusing on topics such as Transparency, Free Access, Security, Accountability and Record Keeping, Leadership, Privacy by Design, PIAs (Privacy Impact Assessments) & Risk Assessments, Data Subject Rights, Vendor Management, and Incident Breach Protocols. By examining these crucial themes, the aim is to gain valuable insights into the practices and strategies adopted by organizations to ensure the responsible handling of data. The participation of multiple organizations in this survey has contributed significantly to our understanding of how local businesses navigate the complex landscape of data management.

Transparency

Transparency is not just a legal requirement but also a fundamental aspect of building trust, ensuring ethical behavior, and fostering positive relationships with customers and stakeholders, especially in the context of privacy regulations. The Think To DO Institute (T2DI) survey results concluded that 50 percent of the think tank session attendees responded partially, 20 percent, no, and 30 percent, yes.

Being transparent about how data is collected, used, and shared builds trust with customers, clients, and partners. Transparency promotes and allows individuals to make informed decisions about sharing their data. Therefore, they can provide informed consent. In many jurisdictions, organizations are required to obtain explicit consent from individuals before processing their personal data for certain purposes. By being open about data practices, organizations can proactively identify potential vulnerabilities and take steps to address them before they escalate into larger issues, thereby reducing the risk of data breaches and regulatory penalties. In the event of a legal dispute regarding data privacy, being able to

⁵ Ibid.

demonstrate transparency in data practices can serve as evidence of compliance with relevant regulations, potentially protecting the organization from legal consequences.

Free Access

The right to free access refers to the fundamental entitlement of individuals to access information, resources, services, and spaces without undue barriers or restrictions. It encompasses various facets of life, including education, healthcare, public services, information, and more. This right is essential for fostering equality, promoting transparency, enabling participation in society, and ensuring that individuals can fully exercise their liberties and make informed decisions. The concept underscores the importance of removing obstacles that might impede people from accessing what they need to thrive and participate meaningfully in their communities.

When assessing this concept in organizations, the focus relies on whether the organization is facilitating and providing free of charge, information about the form and duration of processing, as well as about the integrity of the individuals' personal data. This will be accessible in a public facing privacy notice either online or offline, but also a privacy notice for employees. From the T2DI survey, it can be concluded that 44.44 percent responded yes; 22.22 percent responded no; 27.28 percent responded partially, and 5.56 percent responded not sure of such free access.

Security

The importance of information security cannot be overstated. Information has become a cornerstone of nearly every aspect of our lives, from personal data to critical systems supporting governments and businesses. Ensuring the confidentiality, integrity, and availability of this information is vital to safeguarding individuals, organizations, and entire societies against a myriad of threats. Information security not only protects sensitive data from unauthorized access, breaches, and cyberattacks but also upholds trust, preserves privacy, maintains business continuity, and fosters innovation. The T2DI survey assessed the core principles of information security, namely information Confidentiality, Integrity and Availability. Results were that Confidentiality reported 50 percent, yes, 50 percent, partially. Integrity reported 57.14 percent, yes; 7.14 percent, no; 28.57 percent, partially; and 7.14 percent, not sure. Availability reported 92.86, percent, yes and 7.14 percent, partially.

Accountability and Record Keeping

Accountability and record-keeping are foundational pillars that uphold transparency, integrity, and responsibility within any system, organization, or society. The meticulous practice of maintaining accurate records serves as a cornerstone for accountability, providing a clear trail of actions, decisions, and transactions. These records not only document the past but also serve as a compass for the present and a guide for the future. They offer insights into the accountability of individuals, organizations, or institutions, enabling the assessment of performance, compliance with regulations, and the identification of areas for improvement. The synergy between accountability and record-keeping is essential in fostering trust, ensuring ethical conduct, and facilitating informed decision-making across various domains, from governance and business to personal interactions.

Leadership

Data protection holds immense significance in leadership management due to the crucial role data plays in decision-making, strategy formulation, and overall organizational success. As custodians of sensitive information, leaders are entrusted with ensuring the security, confidentiality, and ethical handling of data. Effective data protection in leadership management engenders trust among stakeholders, employees, and customers. It safeguards sensitive information from unauthorized access, breaches, or

misuse, preserving the integrity and reputation of the organization. By upholding robust data protection measures, leaders not only comply with legal and regulatory requirements but also mitigate risks associated with data breaches that could lead to financial, legal, and reputational damage.

Assigning a Data Protection Officer (DPO) is a strategic move in compliance with regulations like the GDPR (General Data Protection Regulation). This role ensures that data protection becomes ingrained in an organization's culture, strategies, and operations. The result of the T2DI research reported that 28.57 percent of the respondents have appointed an DPO, 35.17 percent has not appointed an DPO. Meanwhile, 14.29 percent partially appointed an DPO, followed by 14.29 percent that were not sure if an DPO was appointed, and last, 7.14 percent reported that the DPO role was not applicable for their organization.

Privacy by Design

Privacy by Design is a proactive approach that embeds privacy and data protection measures into the design and architecture of systems, products, and processes from their inception. It's a framework that prioritizes privacy considerations throughout the entire development lifecycle, aiming to prevent privacy breaches rather than reactively addressing them. This concept, pioneered by Dr. Ann Cavoukian, promotes the integration of privacy features into the core design, ensuring that privacy is foundational rather than an afterthought.⁶ By implementing Privacy by Design principles, organizations can uphold individuals' rights, enhance trust, and create systems that prioritize privacy as a default setting, ultimately fostering a more privacy-conscious and ethical environment. T2DI survey results concluded that 35.71% of the participating organization has implemented a privacy by design approach, 42.86% has not implemented it. While 14.29% of organizations have partially implementing the approach, 7.14 % reported that they were not sure if the organization has adopted this approach.

PIAs (Privacy Impact Assessments) & Risk Assessments

Privacy Impact Assessments (PIAs) and Risk Assessments are crucial tools in the realm of privacy and data protection. A Privacy Impact Assessment is a systematic evaluation used to assess the potential risks and impacts that a project, initiative, or system may have on the privacy of individuals. It involves identifying and mitigating any privacy concerns or risks associated with the collection, use, and handling of personal data. PIAs aim to ensure that privacy considerations are integrated into the design and implementation of projects from the outset, aligning with regulatory requirements and best practices. On the other hand, a Risk Assessment is a broader evaluation that identifies, analyzes, and prioritizes potential risks to an organization's assets, including but not limited to privacy risks. It encompasses various types of risks, such as operational, financial, legal, and reputational risks, along with privacy-related risks. Risk assessments aid in understanding the likelihood and potential impact of these risks, allowing organizations to allocate resources effectively to manage, mitigate, or eliminate them. The institute's survey reported that of the participating organizations 28.57 percent of the organizations do conduct a PIA's and risk assessments, meanwhile 35.71 percent reported NO, 21.43 percent reported partially, and 14.29 percent reported that PIA's and risk assessments are not applicable for them.

Data Subject Rights

Data subject rights refer to the fundamental entitlements individuals hold over their personal data within the realm of data protection and privacy laws. These rights empower individuals to exert control, transparency, and autonomy over the information that organizations collect, process, and store about

⁶ Cavoukian, Ann, PhD, *Privacy By Design*, Information and Privacy Commissioner, Ontario, Canada. 2011

them. Common data subject rights, often enshrined in legislation such as the GDPR, CCPA, LGPD (BRAZIL) and also the Landverordenening Bescherming Persoonsgegevens in Curacao include:

- Right to Access
- Right to Rectification
- Right to Erasure (Right to be Forgotten)
- Right to Restriction of Processing
- Right to Data Portability
- Right to Object
- Rights Related to Automated Decision

Respondents of the T2DI survey reported that 42.86 percent of the participating organizations do provide individuals with information about the processing of their personal data, at the time of collection, and upon request. Meanwhile 14.29 percent reported that they do not provide individuals with this information. 28.57 percent reported that they partially provide individuals with their information and 14.29 percent reported that this is not applicable for their organization.

Vendor Management

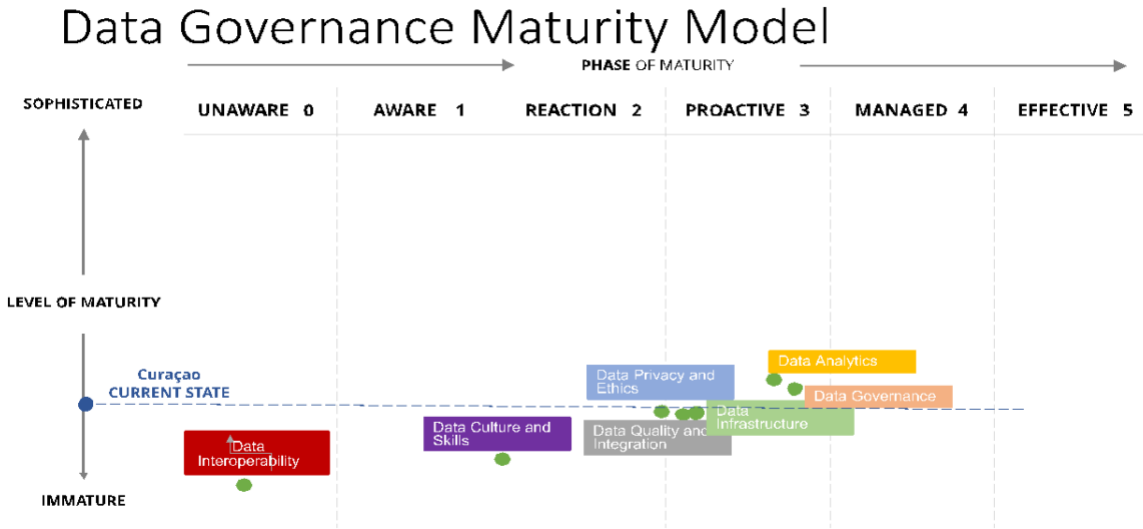
Vendor management is a critical facet of organizational operations that revolves around overseeing relationships and interactions with external suppliers, partners, or service providers. Its significance lies in ensuring that these external entities align with an organization's goals, values, and standards while delivering quality goods or services. Effective vendor management encompasses various aspects such as risk mitigation, cost efficiency, quality assurance, compliance and ethics, Innovation and collaboration, resilience and business continuity. The survey results conclude that 57.14 percent of the respondents stated to have a vendor management system in place, while 14.29 percent stated to have not have a vendor management system. While 7.14 percent partially has a vendor management system in place, 14.29 percent stated that they were not sure, and 7.14 percent stated that a vendor management system was not applicable for them.

Incident Breach Protocols.

Incident and breach protocols are foundational elements in the realm of data security and organizational resilience. They provide a structured framework that guides organizations in responding effectively to security incidents and data breaches. Security incidents encompass a range of events, from unauthorized access to data or systems to malware infections or physical security breaches. Breaches involve the unauthorized access, disclosure, or compromise of sensitive information, often leading to potential harm or misuse of data. Effective incident and breach protocols are crucial for several reasons such as a timely response, compliance and legal obligations, damage control and mitigation, communication strategies, learning and improvement. The T2DI survey reported that 50 percent from the participating organizations stated to have an incident and breach protocol in place, meanwhile 28.57 percent has not. Meanwhile 21.43 percent stated to have partially implemented an incident and breach protocol.

As stated earlier, data maturity encompasses the above listed key aspects. Data policy frameworks maturity is measured by whether the entity, whether private or public, has developed the necessary practices in each of the areas. As a result of the survey and individual interviews with companies across sectors in Curaçao, a representative baseline level of Data Governance Maturity has been identified. Based on the scores for each key area of Figure 2, the graph below shows the distribution and basic maturity level of Curaçao. At best, the level of maturity is at the level 2 of the maturity scale.

Figure 2: Distribution of Curaçao Respondents Data Governance Maturity Survey



Constantly managing and auditing one’s organization is crucial for several reasons, particularly when considering the Gartner Data Maturity Model. Firstly, ongoing management and audits help assess and enhance data maturity, a key factor in achieving organizational objectives. The Gartner Data Maturity Model provides a framework to evaluate an organization’s ability to leverage data for strategic advantage. Regular assessments allow the organization to gauge its progress along the model’s maturity continuum, identifying areas for improvement and potential risks.

Effective data management ensures the accuracy, integrity, and availability of information, laying the foundation for informed decision-making. Additionally, a proactive approach to data management aligns with evolving regulatory requirements and industry standards, reducing compliance risks. The above image illustrates the distribution of Curaçao respondents across the different phases such as data interoperability, data culture and skills, data privacy and ethics, data quality and integration, data infrastructure, data analytics and data governance. In a rapidly changing digital landscape, where data is a critical asset, continuous management and audits are essential to adapt, innovate, and maintain a competitive edge.

2 Data Policy Framework as a driver of institutional policy decisions

The National Data Policy framework plays a crucial role in both public sector and private sector development. It provides guidelines and principles for the collection, storage, sharing, and usage of data within a country, fostering a conducive environment for data-driven decision-making and innovation.

The National Data Policy framework serves as a foundation for data management, governance, and utilization, fostering a data-driven ecosystem that benefits both the public and private sectors. It enables better decision-making, innovation, economic growth, and societal development, while ensuring data privacy, security, and accountability.

Following are some of the most important ways a National Data Policy Framework impacts both sectors.

Public Sector Development:

- **Data Governance:** The framework establishes a structured approach to data governance in the public sector, ensuring that data is managed securely, ethically, and in compliance with relevant laws and regulations.
- **Data Sharing:** It facilitates data sharing among government agencies, enabling better coordination, collaboration, and efficiency in delivering public services. This promotes interoperability and reduces redundancies.
- **Evidence-based Policy:** By promoting data-driven decision-making, the framework enhances the formulation and implementation of evidence-based policies, leading to more targeted and effective public interventions.
- **Transparency and Accountability:** The framework encourages transparency and accountability in the public sector by defining standards for data disclosure, allowing citizens to access and analyze government data, thereby fostering trust and citizen engagement.

Private Sector Development:

- **Data Accessibility:** The framework outlines guidelines for data accessibility, making relevant data available to the private sector for analysis and research. This facilitates market research, product development, and innovation.
- **Data-driven Business Strategies:** The framework encourages businesses to adopt data-driven approaches, enabling them to make informed decisions, identify market trends, understand customer behavior, and develop competitive strategies.
- **Data Privacy and Security:** The framework ensures the protection of personal and sensitive data, giving confidence to individuals and businesses that their data will be handled responsibly. This enhances consumer trust and promotes the growth of digital services.
- **Data Collaboration:** It promotes partnerships and collaborations between the public and private sectors, allowing data sharing for mutual benefits. Such collaborations can lead to the development of innovative solutions and services that address societal challenges.

By creating an integrated system that harmonizes the data flow across the public and private sectors by way of responsible guardrails, more transparency and data availability will exist. Not only will the trust among users rise but also the importance of data-driven decisions will be validated.

2.1 What is currently in place

At the local level, although there have been efforts to develop policy over several years and by way of several governments, this has not yet been actualized.

By law at the formation of Island Curaçao in 2010, the Ministry of Governance, Planning and Public Services was given the task of managing data across all ministries of government.

As for Curaçao, the *National Ordinance on Data Protection* (NODP) has been in effect as of October 1, 2013. This ordinance sets out general principles governing the processing of an individual's personal data and the rights of the person concerned. The ordinance also sets out rules regarding liability for damages incurred by the person concerned. Personal data may only be processed if, for example, the person concerned has unambiguously given his consent; it is necessary for compliance with statutory obligations or for the correct execution of a task regarding public law.⁷

The *Personal Data Protection Board* in Curaçao was established in January 2022.⁸ However, the Board is not yet actively supervising compliance with the rules set out by the NODP. Nonetheless, complaints can already be lodged with respect to non-compliance of the NODP. As part of exercising its supervisory role, the members of the Board have far-reaching powers, such as, but not limited to, the right to demand information and the right of entry into buildings without prior consent.

Since 2019, the scope and effect of the Consensus Kingdom Law has been debated both in the Kingdom legislative chambers and in each of the countries' parliaments. To date there is no clarity as to the impact of a single country's non-agreement with the possibility to assign powers to Dutch bodies in a consensus kingdom law, which can then have an effect and be applicable in the legal systems of the Caribbean countries. This can also have effects on the implementation of a national data framework policy.

2.2 What are some concrete and actionable suggestions

Building and maintaining a data governance framework is a dynamic, inclusive, ongoing and iterative process. It can be viewed as the technology and data architecture that plays the crucial role of data governance. It is driven by prioritized business and societal objectives and desired outcomes, and is delivered with measurable outcomes and a refined roadmap.

Some concrete and actionable suggestions:

1. Draft proposed Data Governance Framework policy and approve modifications to the more limited policy framework that has been adopted but not implemented.
2. Define and adopt the goals for the public and private sectors
 - Improve data quality, which can lead to more accurate and reliable decision making
 - Increase data security to protect sensitive information
 - Enable compliance and reporting against industry regulations
 - Improve overall trust and reliability of your data assets
 - Make data more accessible and usable, which can improve efficiency and productivity.

⁷ Landsverordening Bescherming Persoonsgegevens, Curaçao, 2013.

⁸ Collegebescherming persoonsgegevens, Curaçao, 2022.

3. Using widely accepted stakeholder involvement strategies, engage stakeholders in identifying and delivering on the knowledge and skills needed to design and build the system. Those strategies are guided by the roles and responsibilities assigned (see 4).
4. Identify and define the following roles and responsibilities:
 - *People* refers to the organizational structure, roles, and responsibilities of those involved in data governance, including those who own, collect, store, manage, and use data.
 - *Policies* provide the guidelines for using, protecting, and managing data, ensuring consistency and compliance.
 - *Process* refers to the procedures for communication, collaboration and managing data, including data collection, storage, protection, and usage.
 - *Technology* refers to the tools and systems used to support data governance, such as data management platforms and security solutions.
5. Develop, adopt and refine the data processes as needed. It is important to establish these processes early to prevent issues or confusion that may arise later in the data management implementation.
6. Implement, evaluate, and adapt your strategy. It must be noted that this is a weak point in most adoption cycles. If not built into the implementation plan, the adoption will fail. All systems require monitoring and review. Regularly monitoring and reviewing the data framework strategy will ensure that it is meeting the national goals and public and private business objectives.

The long-term implementation goal is continuous improvement of the use of data within the society to become a resilient society with resilient citizens who make data-driven decisions in order to thrive.

Continuously evaluating the defined goals and objectives, and adjusting as needed, will allow the data governance framework to evolve and adapt to the changing needs of a digital society. Continuous improvement will enable the data governance framework initiative to stay relevant and deliver maximum value to the society.

3 Fundamental Digital Systems; The development of a modern digital system

A digital system is described as digital hardware and software components (internal and external) used to transform data into a digital solution. Digital systems are all around us in the form of computers, smartphones, scanners, cash registers and digital ticket readers. Digitization gained popularity in the late 20th century with the advent of personal computing and the internet. These technologies made it possible to convert many different forms of information, such as text, images, audio and video, into digital forms.

The process of digitization has revolutionized communication and commerce and has had a profound effect on nearly every aspect of modern life. Digitalization is a continuously transformative process and requires constant vigilance and adjustment.

3.1 Adoption of digital transformation

Digital transformation and adoption of the cloud may seem like technical projects, but at their core, both are complex change management efforts involving multiple stakeholders and partners, moving in concert to deliver business and technical change. When they move in unison, the effect on the organization is a game changer.

The scope of digital transformation lies in the speed, scale and flexibility of the process. The acceleration of digital transformation projects magnifies the threats and challenges public and private institutions face. Navigating complexity and siloed mindsets continue to be at the top of the list of challenges for most organizations. Applying change management with a light on implementation complications also remains a focus and raises the importance of creating a culture of continuous learning. Upskilling or reskilling the workforce is important for the continuous flow of transformation successfully with fewer hiccups along the way.

The 2020 Covid-19 pandemic sped up digital transformation especially in economies or industries that had been lagging behind, but the adoption process locally still remains slow.

In 2023, organizations continued to focus on improving the customer experience and increasing engagement. After that, companies have a long and varied agenda. As in previous years, many organizations worked at reducing operational inefficiencies by addressing legacy IT systems. Their aim was to transform business processes and increase digital innovation. This reflected the urgent need to gain flexibility and resiliency via digital transformation strategies.

Each entity is engaged at some level of the transformation journey: Replace or upgrade legacy IT systems, reduce operational inefficiency, improve customer experience and engagement, bolster cybersecurity, introduce new products and services, introduce new business models/revenue streams,

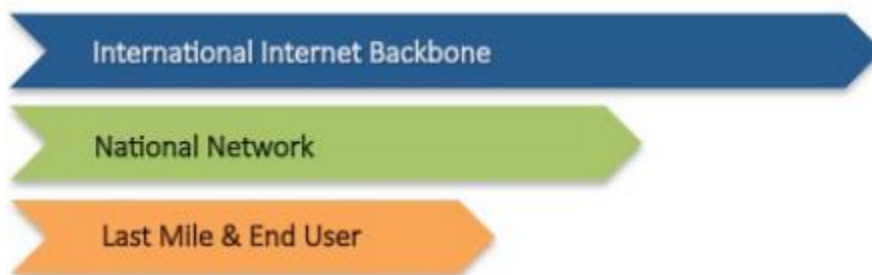
increase/achieve innovation, improve employee experience, increase speed to market of existing products or services, and transform existing business processes.⁹

A fundamental digital system is the foundation of the transformation to a modern digital landscape for the community to utilize in their daily lives by way of universal access. Research on Digital Systems conducted by the NIIS, indicated that the following are the fundamental Digital Systems:¹⁰

- Connectivity (internet coverage that is accessible and affordable) There should also be choice, not monopoly
- Digital Identity
- Digital payment system

3.2 Current State of Connectivity

Most countries, including those in the Caribbean, consider the Internet a critical driver of economic and social development. Therefore, there are continuous efforts to reduce the digital divide in terms of access and quality of Internet access, and to facilitate parties developing and providing IT-services in order to continue their advance toward the construction of inclusive information societies. The state of Internet access and services in the region can be analyzed by examining critical infrastructure elements of the Internet value chain as depicted below.



The primary function of **the international internet backbone** is to facilitate the exchange of data and internet traffic between different regions and countries¹¹. It acts as the backbone for global internet connectivity, allowing data to traverse long distances between continents.

The **national network** serves as the intermediary layer between the international backbone and the local networks. It facilitates the routing of internet traffic within a country, ensuring that data can travel efficiently between different regions.

The **last mile** is crucial because it is the link that delivers internet services directly to end users. This can include various technologies such as fiber optics, DSL (Digital Subscriber Line), cable, wireless, or satellite connections. The end user, in this context, refers to individuals or organizations accessing the internet for various purposes, such as browsing, communication, and online services.

⁹ <https://www.teksystems.com/list/transformation>

¹⁰ *Unravelling the Complexities of National Data Exchange Networks*, Nordic Institute for Interoperability Solutions, NIIS, March, 2023.

¹¹ Coffin, Jane; Fonseca-Hoeve, Bionda; Kende, Michael; Marius, Michele and Osepa, Shernon. *Unleashing the Internet in the Caribbean, Removing Barriers to Connectivity and Stimulating Better Access in the Region*, February, 2017.

According to the *Curacao National Export Strategy – IT services strategy 2022-2027*, Curaçao has a well-developed ICT infrastructure. Several submarine fiber optic cables land on the island, providing international capacity and high-speed links, making the country one of the best connected in the region.



Figure 3: Submarine Cable Map of the Caribbean

Although most countries have two or three cables, Jamaica and Trinidad and Tobago each have five, and Curaçao has six, as seen in the table below¹². In the case of Jamaica and Trinidad and Tobago, their considerably larger populations relative to other countries in the region make them key anchor points, as it is expected that they will generate significantly more traffic, thereby improving the cost recovery and profitability of the cables. In the case of Curaçao, it has established itself as a hub for submarine connectivity.¹³

Curaçao currently has internationally accredited Tier III and Tier IV data centers, and the Tier IV center is one of only 11 in the world.

Country	# of Landing Points	Submarine Cable Systems
Bahamas	3	ARCOS, Bahamas Domestic Submarine Network (BDSNi) and Bahamas Internet Cable System (BICS)
Barbados	2	Eastern Caribbean Fiber System (ECFS) and Southern Caribbean Fiber (SCF)
British Virgin Islands	3	Caribbean-Bermuda U.S. (CBUS), East-West, and Pacific Caribbean Cable System (PCCS)
Curaçao	6	Alonso de Ojeda, ARCOS, Americas-II, ECLink, Jerry Newton and PCCS/Alonso de Ojeda II
Dominica	2	Eastern Caribbean Fiber System (ECFS) and Southern Caribbean Fiber (SCF)
Grenada	2	Eastern Caribbean Fiber System (ECFS) and Southern Caribbean Fiber (SCF)
Haiti	2	Bahamas Domestic Submarine Network (BDSN), Fibralink
Jamaica	5	ALBA-1, Cayman-Jamaica Fiber System, Colombia-Florida Subsea Fiber (CFX-1), East-West and Fibralink

¹² Ibid

¹³ <https://www.submarinecablemap.com/landing-point/willemstad-curaao>

St. Maarten	2	Eastern Caribbean Fiber System (ECFS), Sint Maarten Puerto Rico Network One (SMPR-1)
Suriname	1	Suriname-Guyana Submarine Cable System (SG-SCS)
Trinidad and Tobago	5	Americas-II, Eastern Caribbean Fiber System (ECFS), ECLink, Southern Caribbean Fiber (SCF), Suriname-Guyana Submarine Cable System (SG-SCS)

The Caribbean’s Changing Submarine Cable Space

In 2013, Columbus Networks Limited (CNL) and Cable & Wireless Communications Plc (CWC) established a joint venture, CNL–CWC Networks Ltd., in order to provide “expanded wholesale bandwidth capacity to global, regional and local communications companies in the Caribbean and Americas Region”. However, in March 2015, Cable & Wireless Plc (CWC’s parent company) bought Columbus International (CNL’s parent company), and six months later CWC was bought by Liberty Global Plc, a British broadband operator and one of the largest cable firms in the world, for USD 5 billion.¹⁴ Similarly, Digicel, the largest mobile/cellular operator in the region (by market share), has been investing in its submarine cable system. In 2014, it bought the submarine cable assets of *Global Caribbean Fiber and Global Caribbean Network* to create a fiber-optic cable network of approximately 3,100 km providing capacity from Trinidad in the southern Caribbean to Puerto Rico in the north. The firm has approval to build out networks connecting the Bahamas, Haiti and Jamaica and connecting Guyana.¹⁵

Last Mile to End User

The “last mile” refers to the communications link between the customer and the closest local exchange, base station, or wireless node. It is where the greatest service differentiation takes place and, therefore, is where competition is likely to be strongest. Note that none of the countries in the region or this study have required their incumbent fixed-line operators to offer wholesale rates to other Internet service providers (ISPs) for access to their last-mile networks—an arrangement known as “local loop unbundling”.

Medium	Technology	Transmission Speed (Max)	Comments
Copper lines	ADSL/ADSL2	12 Mbps	ISPs, e.g., LIME (regional), Telesur (Suriname), UTS, Telem (St. Maarten) and Marpin (Dominica)
Wireless	GPRS	171 kbps	Low speed connectivity ideal for short message services (SMSs)
	EDGE	384 Kbps	Most mobile networks support EDGE
	Wi-Fi (2.4/5GHz ISM bands)		Antigua Computer Technology, DEKAL Wireless (Jamaica), Neptuno and WISCNet (Puerto Rico)
	HSPA/HSPA+	56 Mbps	Upgraded base stations (mostly in large urban areas) of some mobile networks
	WiMAX	40 Mbps– 1 Gbps	Jamaica Government (TV White Space), CCT, Scarlet (WiMAX)
	LTE	100 Mbps	Spice Mobile (Grenada), Flow/LIME, Digicel, BTC (Bahamas), Smart (Belize), UTS/Chippie (Curaçao) , Kia (Bonaire), Only (Martinique), and TSTT/Bmobile (Trinidad and Tobago)
Coaxial cable	Broadband over coax cable	100 Mbps	Bahamas Cable, Flow (Antigua, Barbados, Curaçao , Grenada, Jamaica, St. Lucia, St. Vincent and the Grenadines, and Trinidad), and Digicel (Anguilla, Dominica, Jamaica, Montserrat, Nevis, and Turks and Caicos Islands)

¹⁴ Unleashing the Internet in the Caribbean Removing Barriers to Connectivity and Stimulating Better Access in the Region, Curacao, February, 2017.

¹⁵ Ibid.

Fibre-optic cable	FTTx/xPON	>100Mbps	In countries such as Barbados and Jamaica, Flow has been deploying fiber to the home, with maximum download speeds of 300 Mbps. Digicel is deploying fiber networks in Barbados, Haiti, Jamaica and Trinidad
--------------------------	-----------	----------	---

Fixed-line network operators tend to have a monopoly on the last mile, which is generally considered a barrier to market entry. This barrier to entry reduces take up for business customers located in the major urban areas where copper cable has been deployed.

Transmission Speeds

According to the *International Telecommunication Union* (ITU), the standard for broadband is a transmission speed of at least 1.5–2.0 Mbps. Other organizations, such as the Organization for Economic Co-operation and Development (OECD), have adopted the following minimum speeds for wired and wireless broadband Internet services.

- Basic broadband: 256 kbps (download), 128 kbps (upload)
- Advanced broadband: 2 mbps (download), 512 kbps (upload)
- Total broadband—a service that can support all applications available on the Internet: 10 Mbps (download), 768 kbps (upload).

The figure below shows a rolling average of actual upload and download speeds for fixed broadband (wired and wireless) networks over a 30-day period ending in February 2015 in the countries under review (with the exception of Sint Maarten, for which data was not recorded). The data was sourced from speed tests that were conducted; these were carried out within 300 miles of the server.¹⁶

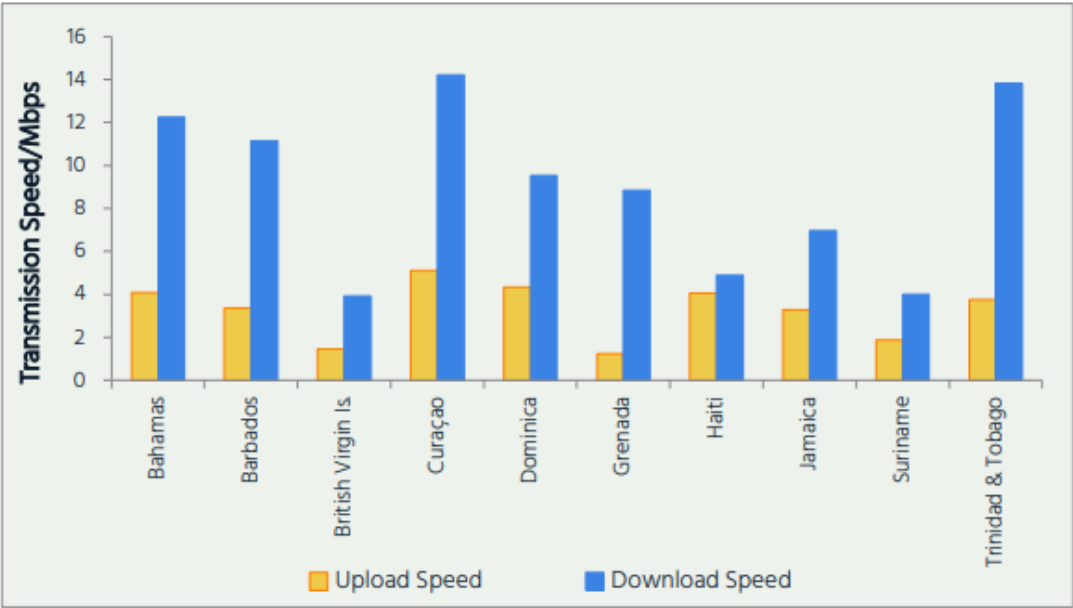


Figure 4: Fixed Broadband network speeds 2015

As can be seen, there is a wide disparity in transmission speeds across the region. The slowest upload and download speeds were recorded in the British Virgin Islands (1.46 Mbps and 3.92 Mbps, respectively), while the fastest upload and download speeds were recorded in Curaçao (5.11 Mbps and

¹⁶ Ibid. Page 30

14.21 Mbps, respectively). Even the speeds in Curaçao are below the global average of 10 Mbps (upload) and 22 Mbps (download). The information above is based on information from 2015. No newer information comparing speeds across Caribbean countries listed is available at the time of this publication.

According to the 2017 CBS publication, the most recent household survey, revealed that 51.6 percent of the households of Curaçao have a computer which everyone in the households has access to and can use. The percentage of households with shared internet access is higher at 64.5 percent.¹⁷

It can be deduced that 35.5 percent of households do not have access to the internet at home. Of those who do not have access more than half indicate that the main reason is the high cost of internet connection, followed by the high cost of computers. Of that 35.5 percent, the reasons given according to a survey by the CBS were as follows:

Reason household does not have internet	
Due to the high cost of internet connections	51.30%
Due to the high cost of computers (desktop PCs, laptops, tablets and similar)	40.70%
We do not need internet	31.80%
We have access to internet elsewhere	17.90%
Due to lack of trust, know-how and skill to use the internet	9.80%
There is no internet infrastructure in our neighborhood	8.50%
We worry about privacy and security	7.90%
There is internet infrastructure, but it does not meet the needs of our household	4.30%
Other reason	17.30%

Figure 5: Household with shared ICT Computer Access

The cost of internet access can have significant effects on socio-economic and educational aspects in countries where the cost is high or there is a prevalent monopoly. In the past six years since this survey, the internet landscape has changed considerably which requires a repeat survey to get more accurate household data.

Socio-Economic Impact

The cost of internet access often widens the gap between those who can afford it and those who cannot, exacerbating existing socio-economic inequalities. Limited internet access may also hinder individuals and businesses from accessing crucial information, job opportunities, and engaging in the local or global markets, impacting economic opportunities.

Education Impact

Students with limited internet access face challenges in accessing online educational resources, hindering their learning experience. The reliance on online learning platforms is growing, especially after the COVID-19 pandemic, but high internet costs may impede students' ability to participate in e-learning, affecting educational progress. Affordability plays a crucial role in educational disparities, with students from lower-income families facing challenges in accessing online tools and resources.

¹⁷ https://cuatro.sim-cdn.nl/cbscuracao/uploads/integration_of_ict_in_private_households.pdf?cb=7NdwqBIM

Social Impact

Lack of means for digital communication can play a huge role in diminishing social connection. Limited affordability can impact people's ability to connect with others through social media and other online communication platforms. Reduced internet access may also limit citizens' awareness of local and global events, affecting their access to timely news and information. This however is somewhat mitigated due to the fact that traditional media (TV, radio, newspaper) is still a prevalent source of communication in Curaçao.

Other research studies conducted by the Think To DO Institute related to social cohesion, reveal that little change has occurred in access to the internet.

Government and Policy Considerations

Policy Reforms: Governments may need to implement policies and regulatory measures to reduce internet costs, or stimulate open markets with competing entities. Collaboration between the public and private sectors is crucial to finding solutions that reduce internet costs while maintaining a sustainable telecommunications market.

Recognizing the importance of affordable connectivity for socio-economic development and education and enforcing/supporting that with policies may contribute to a more resilient society. Addressing high internet costs and ensuring affordable access contributes to building a resilient and future-proof society. Affordable, accessible internet promotes economic inclusivity, fostering innovation and entrepreneurship. Lowering barriers to access prepares a diverse workforce for the skills required in the future job market, enhancing long-term societal resilience.

Moreover, affordable internet access empowers individuals through digital literacy, supporting social cohesion, and connectivity.

This connectivity also facilitates global participation, allowing effective collaboration and information sharing, and opening Curaçao to regional and global commerce contributing to a more interconnected and resilient economy. Furthermore, investments in digital infrastructure, often required to address internet affordability, lay the foundation for advanced technologies and communication networks. This not only addresses current economic and educational needs but also signifies an investment in the adaptability and future success of society.

3.3 Current state of digital payment system

Developing a national payment system is an ongoing process. The planning and implementation of payment system development is a difficult task due to the complexity of, and the varying approaches to, reforms. The authorities that promote new initiatives in their national payment systems generally look to other countries and to the *Committee on Payment and Settlement Systems (CPSS)*, the *International Monetary Fund (IMF)*, the World Bank and other international financial institutions for information, advice and assistance regarding how best to plan and implement reforms in such a system.

A national **Retail payment system** primarily focuses on retail transactions, which typically involve payments between individuals and businesses for goods and services.

A **“Unified Payment System”** or a **“Multi-Purpose Payment System”**, in addition to handling retail

transactions, is designed to facilitate payments related to government services and utilities, such as taxes, social benefits, fines, and public transportation fees. It extends its functionality to encompass payments made to or by government agencies for various public services.

According to *CurFinTech Association* representatives, the scope of implementation in Curaçao is not inclusive. The local/retail payment rails are managed by the country's regulated banks and are only accessible by the 'banked' public. Without a bank account linked to a bank card, a person cannot make use of these rails.

There is NO 'unified payment' system locally as described above. All utility as well as government payments go through the banking system.

The current state of the national payment system is limited to the banked customer. As this has been historically the case, real tech innovation in payments and payment-rails have been in the hands of the regulated banks. While economies of scale define the rate of return on these innovation investments, It can be safely stated that the local payment rails are just now catching up with the introduction of the instant payment network, where settlement of retail bank transfers are immediate. This brought about a change in digital transfers.

This new improved rail is also only accessible to the banked. Therefore, main challenges to full implementation include: Not yet inclusive to non-banks / payment processors / not accessible to the unbanked.

The existing infrastructure hinders financial transactions and digital payments. Although the IP network has improved settlement drastically, frictionless person to person payments are still not possible, real innovation towards direct merchant payments is not possible yet and in a certain way monopolized by the *Central Bank of Curaçao and St. Maarten* (CBCS) due to the inaccessibility of fintech's to yet operate on the network. The CBCS currently is the regulator (provides rules and payment regulations / legislation) but also is the implementer and operational party running the network. This construction will hamper continuous innovation and progress. The CBCS should be the facilitator to and provide room for, and manage sandboxing for fintech innovators to bring solutions. That is the best way real innovation can be developed and brought to the public.

Initiatives such as the managed introduction of a Central Bank Digital Currency (CBDC) will bring real innovation to the payments environment of the island. The benefits of a CBDC are tangible and quantifiable. According to the Fin Tech companies, instead of investing in the production of a new fiat currency, a better solution would be to introduce a digital currency that is backed by and managed by the Central Bank. A digital currency will: (to name a few advantages)

- Reduce cost of producing, managing fiat cash (for the CBCS as well as the commercial banks themselves),
- No more wear and tear to cash dispensing and payment machines,
- Everyone, including the 'unbanked', that has a cellphone can easily receive and send the digital money.
- Taxes can easily and directly be charged on all transactions (i.e. OB)
- Thresholds on transactions can easily be instituted to prevent / combat unusual transactions

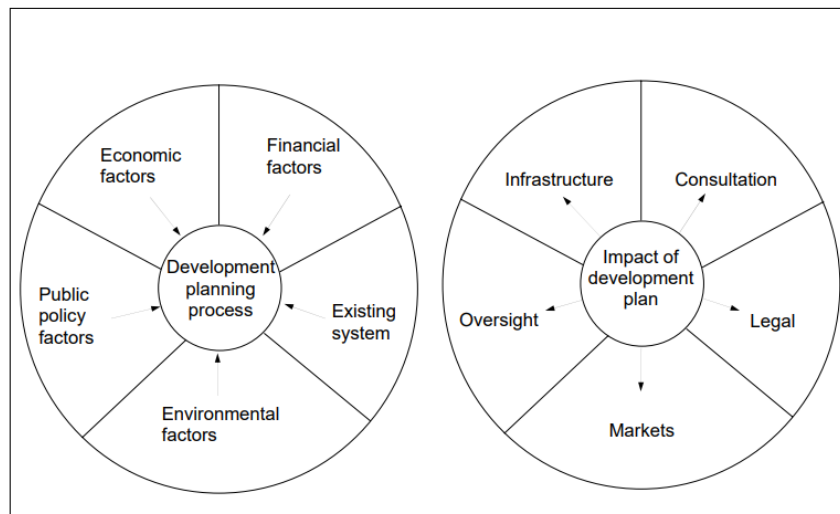
The incumbent banks are just followers by regulation of the CBCS and will not invest if they do not have/cannot reach critical mass for a successful initiative. That is unlikely as they cannot cater to the

unbanked. There are various local fintech companies with great innovative solutions that are hampered by the fact that they need to become / apply for a banking license to exploit their innovations.

The Cur FinTech initiative was originated from the lack of and the need to form a body / entity as a sparring partner for the policy making of the CBCS, as well as addressing the need to create awareness in the local sector of fintech companies that have the potential to deliver solutions. This Cur FinTech constellation of companies is a collaboration amongst Profound, IBIS Management & Associates, CX Pay and Ictual that are all private companies. There are no public companies nor banks.

Development Factors

Figure 6: Development Planning Process



The four general factors influencing national payment system development could be grouped together as

- environmental factors
(Influences likely acceptance of particular development initiatives)
- economic factors
(Influences the need/urgency of payment service and capabilities of the country)
- financial factors
(Cost to benefit ratio influences likelihood of implementation)
- public policy factors
(Interests of the various stakeholders influence the direction in which the national payment system develops through their effects on the demand for, supply of and market arrangements for payment services.)

Given the circumstances related to development of the payment system, it is difficult to gauge the state of these 4 factors in Curaçao. What can be observed is multiple initiatives by various stakeholders that leads to fragmentation rather than a **Unified Payment System**.¹⁸

There are still questions that need to be answered related to the Technology and Infrastructure being considered or utilized in the implementation of the national payment system. Further questions remain related to the measures to protect security and privacy of transactions and user data, and the

¹⁸ *Payment Systems Worldwide, A Snapshot*, World Bank Group. September, 2018.

importance of an independent entity that functions as owner and governing body of the system. Finally, there always remains the important concern of who will guard against fraud and cyber threats.

Financial Inclusion, Education and Awareness

Equal access and equality of access is imperative to a national payment system that promotes financial inclusion and accessibility to a wide range of users, including those in underserved areas. There needs to be an education and awareness component to educate the public and businesses about the benefits and usage of the new payment system. At this time there is no evidence of these components.

3.4 Current state of Digital identity

Digital identity is typically defined as a one-to-one relationship between a human and their digital presence. A digital presence can consist of multiple accounts, credentials, and entitlements associated with an individual. Currently, there is not a standard set locally for what are the official digital identity formats. Various public entities on their own have selected the use of four digital formats as current practice: personal ID (cedula), passport, drivers' license, tax number (crib number), Chamber of Commerce number (KvK), Social Security number (SVB). In September 2022, it was reported that the Multi Tax Solution (MTS) and Multi Collection Solution (MCS) presented by BearingPoint in 2015 were presented to the government but the MTS has not been implemented and MCS has not been completely implemented. There are no standard formats noted in the private sector.

Good digital ID is a new frontier in value creation for individuals and institutions around the world. One of the key advantages of digital identity verification is that it can be done remotely, which became particularly important during the COVID-19 pandemic. This form of ID means that individuals can verify their identity without having to physically visit a location, which can save time and money and increase personal data security.

There are requirements for a good digital ID as Digital Identity. These requirements will retire previous "level of assurance requirements" but will use a similar numerical leveling that ensures unique identifiers for individuals. These requirements must be set in the national data framework and must include:

1. Identity proofing process (IAL)
2. Authentication process (AAL) and
3. Strength of an assertion in a national environment (FAL)

The separation of these categories provides agencies flexibility in choosing identity solutions and increases the ability to include privacy-enhancing techniques as fundamental elements of identity systems at any assurance level.

The decision tree below highlights the risks that need to be managed for a digital identifier service offering, be it at the national, public or private services levels.¹⁹

¹⁹ Digital Identity Guidelines, IST Special Publication 800-63-3, US Department of Commerce, June, 2017.

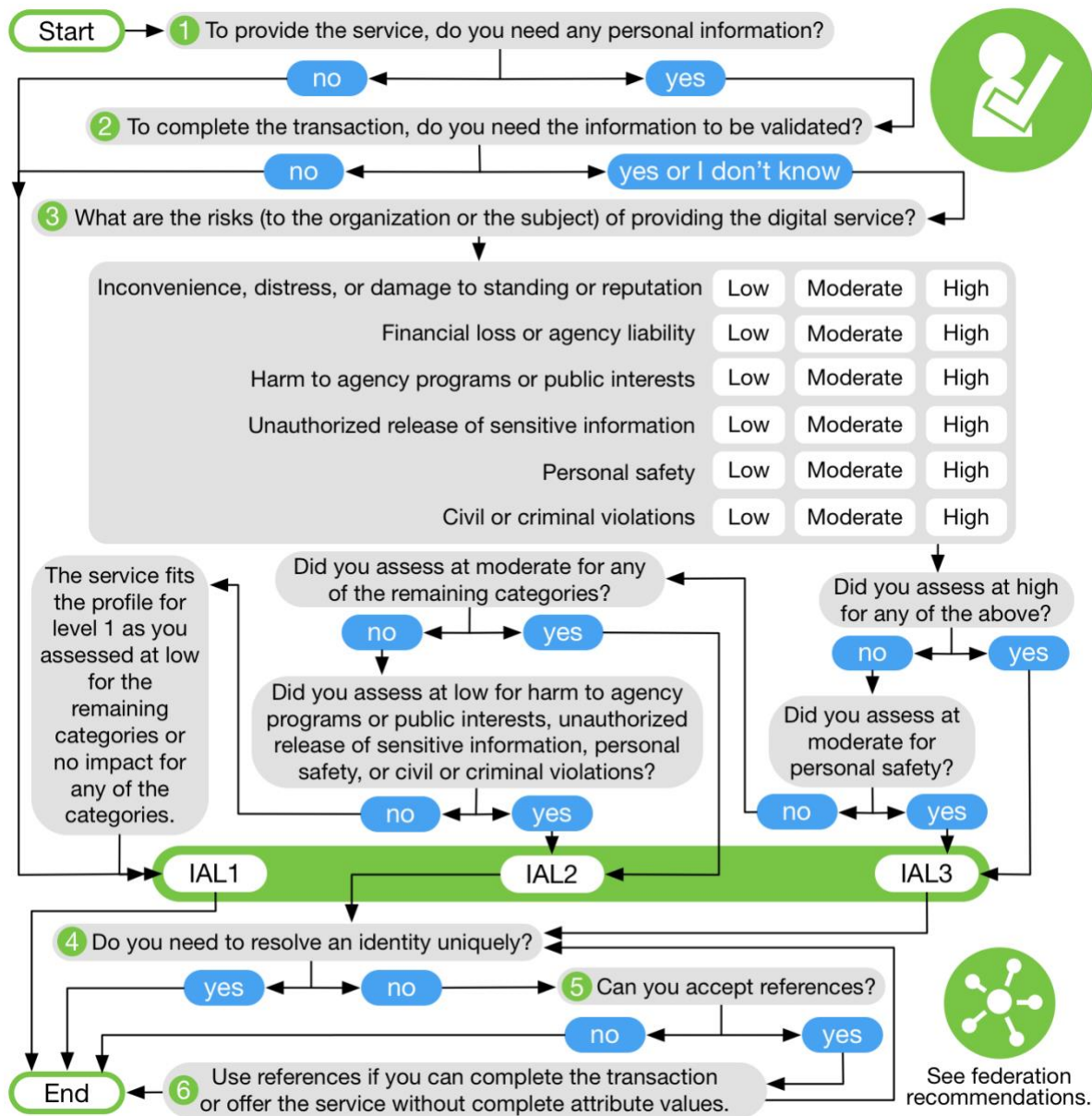


Figure 7: Decision Making Tree For Determining Digital Services Security

At the time of this writing, there are no laws, policies or regulations in place for the development of unique digital identities at the country level for either public or private use.

Global best practices are to comply with security and privacy standards as referred to NIIS Framework in previous Chapters. Federation is a keystone in the ability to enhance the privacy of the national government's constituents as they access valuable government digital services.

4 Data Policy Framework Elements

Building a National Data Policy Framework is intrinsically linked to the importance of data-driven decision-making. This framework sets the governance structure, strategic approach, and ethical principles for efficient data management, emphasizing, confidentiality, integrity and availability.

It ensures data privacy and ethics while promoting data sharing and collaboration. Security measures protect data, and the framework fosters innovation and accountability. By adhering to this framework, governments are equipped to make evidence-based decisions that positively impact policy, strategy, and society.

4.1 CIA Triad

The three letters in “CIA triad” stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.²⁰

The confidentiality, integrity, and availability of information is crucial to the operation of a business, and the CIA triad segments these three ideas into separate focal points. This differentiation is helpful because it helps guide security teams as they pinpoint the different ways in which they can address each concern.

Ideally, when all three standards have been met, the security profile of the organization is stronger and better equipped to handle threat incidents.

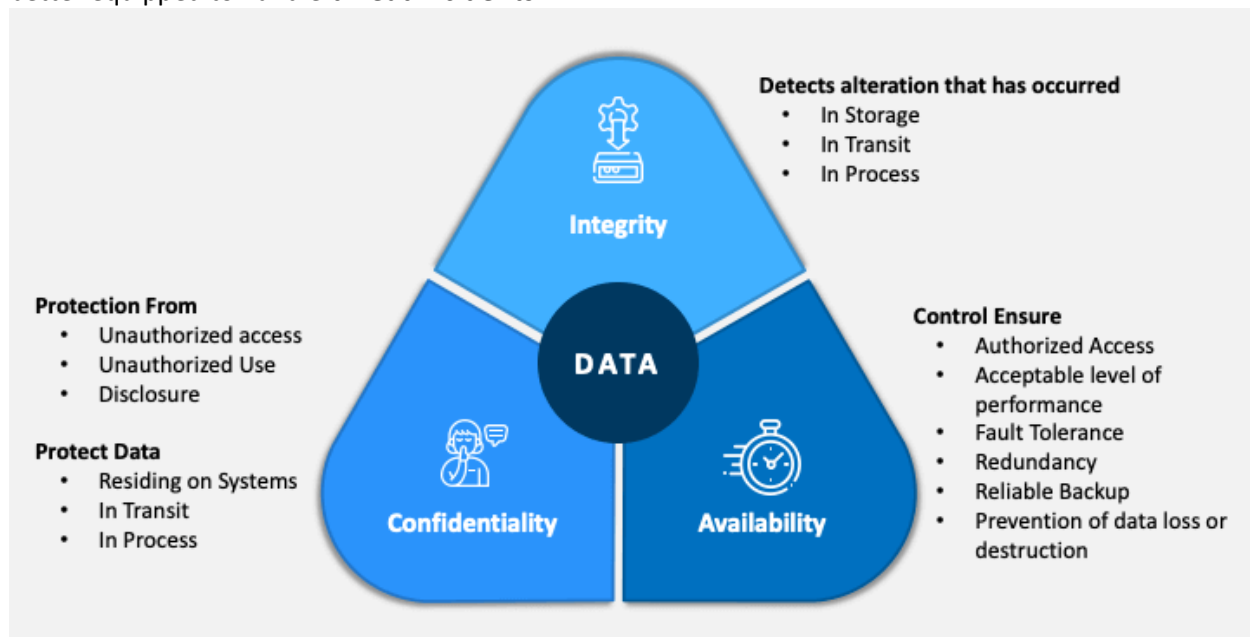


Figure 8: CIA Triad

²⁰ <https://www.fortinet.com/resources/cyberglossary/cia-triad>

4.2 Data confidentiality

Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

Within the context of a National Data Policy Framework, data confidentiality plays a vital role in data-driven decision-making. To encourage data sharing and collaboration, it's necessary to have robust mechanisms in place to protect sensitive information. Data privacy regulations and ethical considerations are critical to maintain public trust and ensure that individuals' rights are protected.

4.3 Data integrity

Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable. Inaccurate or corrupted data can lead to misguided decisions.

A National Data Policy Framework should address data quality and accuracy by establishing data validation procedures, data cleaning processes, and quality control mechanisms. Decision-makers rely on data that is consistent and trustworthy.

A method for verifying integrity is non-repudiation, which refers to when something cannot be repudiated or denied. For example, if employees in your company use digital signatures when sending emails, the fact that the email came from them cannot be denied. Also, the recipient cannot deny that they received the email from the sender.

4.4 Data availability

Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization.

Data availability is crucial for making informed decisions. A National Data Policy Framework should prioritize ensuring that relevant data is accessible, both in terms of its existence and ease of retrieval. Without available data, the decision-making process can be impaired or misinformed. It's essential for government agencies, organizations, and institutions to share their data in a standardized and accessible format to support data-driven decisions. Chapter 5 of this document will expand on the Role of Open Data in National Development.

9.6 Data interoperability

Data interoperability is essential for enabling different data sources to work together seamlessly. A National Data Policy Framework should promote standards and protocols that allow various datasets to be compatible and interconnected. Interoperability facilitates data sharing and integration, enabling more comprehensive and holistic data-driven decision-making. Chapter 5 explains further the

importance and components of the European Interoperability framework.

Although Data Interoperability is not an official part of the C.I.A. triad, it is however extremely important as a foundational structure that provides a means of data exchange between systems and between participating parties.

With the rise of Artificial Intelligence (AI) and autonomous technologies, the traditional Confidentiality, Integrity & Availability “C.I.A. Triad” further demonstrates its insufficiency due to its avoidance of a safety component for cybersecurity practices. The C.I.A. Triad does not adequately represent a digital world with embedded technologies (e.g., Internet of Things (IoT) and Operational Technology (OT)) and AI-powered capabilities.

9.6 D.I.E. Triad

The D.I.E. Triad (Distributed, Immutable, Ephemeral) serves as an alternative to the C.I.A. Triad (Confidentiality, Integrity, Availability) that reduces the security burden, enables users to achieve true resiliency, and move towards antifragility.²¹

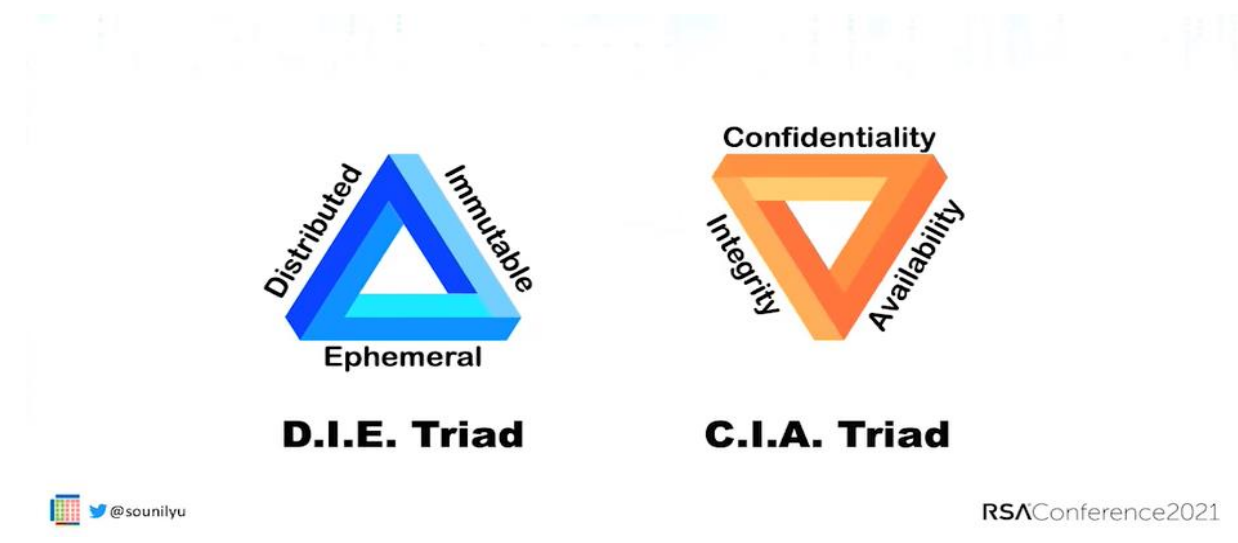


Figure 9: Comparison of the Common Models of Data Security Systems

As more applications, systems and infrastructure are now designed and built in a highly distributed and always available manner, they are highly resilient, fault tolerant, elastic and scalable – in the cloud and/or on-premises. This help addresses the availability aspect of the C.I.A. triad.²²

Because the applications, systems, and infrastructure are created to be immutable, small changes are detected very easily. This removes the need to maintain integrity. Integrity problems occur when there is the ability to make changes, either intentionally or unintentionally, that are very hard to detect. That affected the integrity aspect of the C.I.A. triad.

²¹ https://www.cisa.gov/sites/default/files/publications/Daily_Keynote_with_Sounil_Yu_508pobs.pdf

²² <https://www.bankinfosecurity.com/blogs/new-enterprise-risk-management-strategy-p-3136>

Being ephemeral makes the applications, systems, and infrastructure transient, or short-lived. That disrupts the persistence that a malicious attack requires to affect the confidentiality aspect of the C.I.A. triad and makes the window of opportunity for the attacker much smaller.

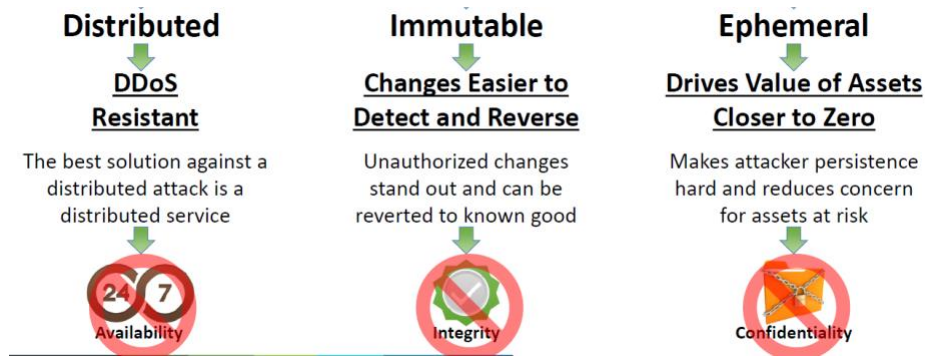


Figure 10: Comparison of D.I.E. to C.I.A.

5 European Interoperability Framework (EIF)

In today's digital world information is stored across multiple information systems owned and maintained by different organizations. In addition to information spreading across multiple organizations, every organization has internally numerous information systems that store information. Most of the digital services and processes require accessing multiple information systems and combining data from different sources – both inside an organization and across multiple organizations. Without connections between different information systems, building digital services would be extremely challenging if not impossible.²³

As described in Chapter 4.5, interoperability is important for enabling information systems to exchange and utilize information. In the context of a National Data Policy, interoperability is not only about technology and technical connectivity. On the contrary, interoperability consists of different layers that also include technology. The European Interoperability Framework (EIF) defines two supporting layers:

1. a background layer, 'interoperability governance'
2. a cross-cutting component of the four layers, 'integrated public service governance'

And furthermore, it defines four layers of interoperability:

1. legal – aligned legislation
2. organizational – coordinated processes
3. semantical – precise meaning of exchanged information
4. technical – connecting information systems and services.²⁴

The model is depicted below:

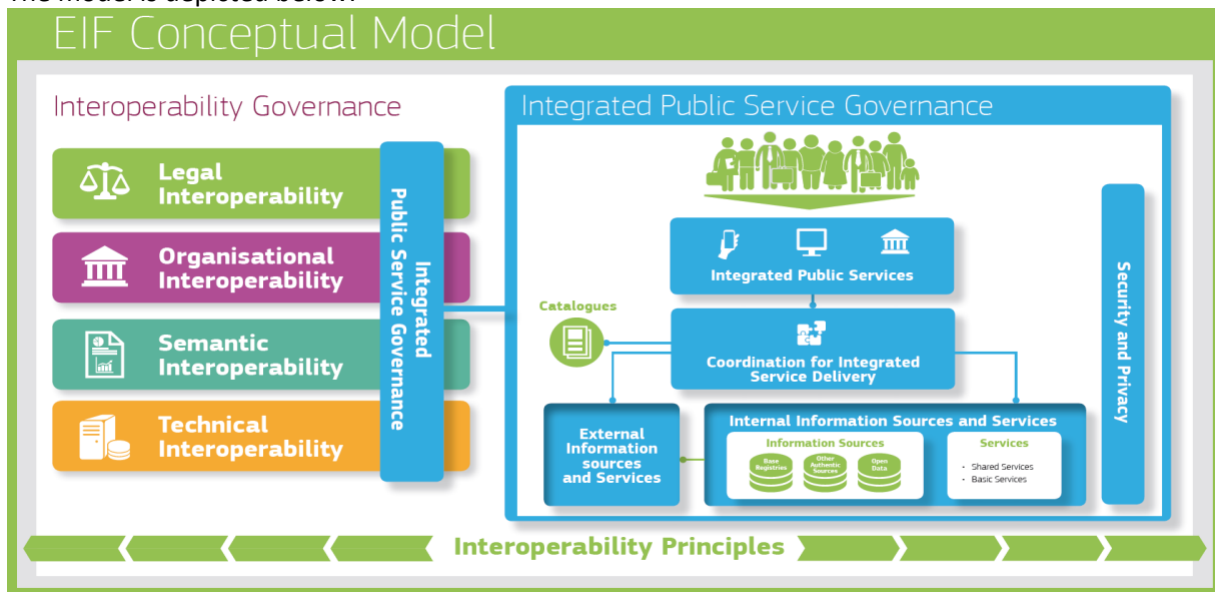


Figure 11: EIF Conceptual Model for Interoperability

²³ <https://www.niis.org/blog/2020/1/20/interoperability-puzzle>

²⁴ <https://inspire.ec.europa.eu/news/new-european-interoperability-framework-eif>

5.1 Interoperability Governance

European public services operate in a complex and changing environment. Political support is necessary for cross-sectoral and/or cross-border interoperability efforts to facilitate cooperation between public administrations. For effective cooperation, all stakeholders must share a vision, agree on objectives and timeframes and align priorities. Interoperability between public administrations at different administrative levels will only be successful if governments give sufficient priority and assign resources to their respective interoperability efforts.

The lack of the necessary in-house skill sets is another barrier to implementing interoperability policies. Member States should include interoperability skills in their interoperability strategies, acknowledging that interoperability is a multi-dimensional issue that needs awareness and skills in legal, organizational, semantic and technical.

Interoperability governance is the key to a holistic approach on interoperability, as it brings together all the instruments needed to apply it. Coordination, communication and monitoring are of the utmost importance for successful governance.

5.2 Integrated public service governance

When multiple organizations are involved, there is a need for coordination and governance by the authorities with a mandate for planning, implementing and operating European public services. Services should be governed to ensure integration, seamless execution, reuse of services and data, and development of new services and 'building blocks'.

Organizations involved in European public service provision should make formal arrangements for cooperation through **interoperability agreements**. Setting up and managing these agreements is part of public service governance.

Agreements should be detailed enough to achieve their aim, i.e. to provide European public services, while leaving each organization the maximum feasible internal and national autonomy. At the semantic and technical levels, but also in some cases at organizational level, interoperability agreements usually include standards and specifications. At the legal level, interoperability agreements are made specific and binding via legislation at EU and/or national level or via bilateral and multilateral agreements.

Other types of agreements can complement interoperability agreements, addressing operational matters. For example, memoranda of understanding (MoUs), service level agreements (SLAs), support/escalation procedures and contact details, referring, if necessary, to underlying agreements at semantic and technical levels.

Since delivering a European public service is the result of collective work with parties that produce or consume parts of the service, it is critical to include appropriate change management processes in the interoperability agreements to ensure the accuracy, reliability, continuity and evolution of the service delivered to other public administrations, businesses and citizens.

All four layers are equally important when building digital services and processes. In addition, challenges on one layer are often reflected on other layers too. An extensive explanation of the EIF can be found in

the interoperability framework document created for the European Union.²⁵ Any country that is interested in improving interoperability within the public sector digitization process, should make note of these interoperability principles.

5.3 Legal interoperability

Legal interoperability is about ensuring that organizations operating under different legal frameworks, policies and strategies are able to work together. This might require that legislation does not block the establishment of European public services within and between Member States and that there are clear agreements about how to deal with differences in legislation across borders, including the option of putting in place new legislation.

The first step towards addressing legal interoperability is to perform ‘interoperability checks’. This involves reviewing current legislation to pinpoint potential barriers to interoperability, such as sector-specific or geographical limitations on data use and storage, diverse and unclear data licensing models, over-restrictive obligations to use specific digital technologies or delivery modes to provide public services, outdated security and data protection needs, etc.

Bearing in mind that European public services are clearly meant to be provided, amongst others, from *digital channels*, ICT must be considered as early as possible in the law-making process. In particular, proposed legislation should undergo a ‘**digital check**’:

- to ensure that it suits not only the physical but also the digital world (e.g. the internet)
- to identify any barriers to digital exchange
- to identify and assess its ICT impact on stakeholders

This will facilitate interoperability between public services at lower levels (semantic and technical) as well, and increase the potential for reusing existing ICT solutions, reducing cost and implementation time.

5.4 Organizational interoperability

This refers to the way in which public administrations align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals. In practice, organizational interoperability means documenting and integrating or aligning business processes and relevant information exchanged. Organizational interoperability also aims to meet the requirements of the user community by making services available, easily identifiable, accessible and user-focused. Different entities may use different business processes, so there will be a need to align their existing business processes or define and establish new ones.

Aligning business processes implies documenting them in an agreed way and with commonly accepted modeling techniques, including the associated information exchanged, so that all public administrations contributing to the delivery of European public services can understand the overall (end-to-end) business process and their role in it.

²⁵<https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail>

5.5 Semantic interoperability

Semantic interoperability ensures that the precise format and meaning of exchanged data and information is preserved and understood throughout exchanges between parties, in other words ‘what is sent is what is understood’. It ensures the ability of information systems and services to exchange and use data in a way that is mutually understandable, even if they are developed independently. It goes beyond technical compatibility and focuses on ensuring a common understanding of the meaning of data and information across different systems, organizations, and domains.

5.6 Technical interoperability

The applications and infrastructures linking systems and services are important to the process. Aspects of technical interoperability include interface specifications, interconnection services, data integration services, data presentation and exchange, and secure communication protocols. The EIF outlines technical principles and standards to ensure that differing IT-systems can interoperate effectively, fostering collaboration and integration across diverse platforms and services within the European Union.

5.7 Netherlands towards Interoperability

The Netherlands has a high e-Government performance, stemming from almost two decades of eGovernment policy. Current policies are the *Digital Government 2017* and the *Digital Agenda 2020*. The *Digital Government 2017* vision paper fosters the digital-by-default approach, elaborating on the need for digital communication between citizens and government, the optimal use of the data by the government and the improvement of the common infrastructure.

The *Generic Digital Infrastructure (GDI)* was a natural evolution of the information infrastructure that was developed under the i-NUP. The infrastructure has matured over the years, and is now a collection of services, provisions, standards, interfaces, authentication mechanisms, base registries for re-use of data and interconnectivity. The operational GDI, to a large extent managed by *Logius* (an agency under the Ministry of the Interior and Kingdom Relations), can be regarded as the foundation of the Dutch interoperability efforts.

The **Dutch National Interoperability Framework (NIF)**, named **NORA (Nederlandse Overheid Referentie Architectuur)**, is intended to give direction and to be a supporting instrument for Public Administrations. It contains policy frameworks and arrangements for setting up the ICT systems of the Dutch government. These frameworks and agreements ensure that these ICT systems work well together and make optimal re-use of existing solutions. NORA also provides principles, standards, and building blocks grouped in various themes at operational level.

In terms of open data, another important example of the Dutch electronic-leading position is *the Open Data Portal*, officially launched in 2011. At the moment, the portal references up to 10,281 data sets, while paying special attention to the quality of the data by monitoring the availability and improving the visibility of the data. The portal offers access to open data, enabling citizens to identify and re-use Government data related to the environment, infrastructure, population, and other statistics.

Additionally, the *European Single Market* drives the need for more cross border exchange of data. Next to initiatives at European Level, Member States sometimes also enter in close cross-border cooperation.

Accordingly, the Netherlands is a member of *EUCARIS* (European CAR and driving license Information System), *ECRIS* (European Criminal Records Information System), and of the *ELRA* (European Land Registry Association) through *Cadastre*, Land Registry and Mapping Agency. Extensive information on how The Netherlands is implementing elements of EIF can be found in supporting document.²⁶

²⁶ <https://joinup.ec.europa.eu/sites/default/files/inline-files/Netherlands%20Factsheet%20Validated.pdf>

6 Data concepts and the Role of Open Data in National Development

At a time when citizens, consumers and employees are all demanding greater transparency from public institutions, open data is becoming vital for successful government at a national level. However, many countries are not yet fully embracing open data. That is the conclusion of the *2022 Open Data Maturity Report*, published in December by the European Commission.²⁷

The *Open Data Maturity (ODM) Report 2022* records the progress achieved by EU Member States as they push forward open data publication and reuse, as well as the different priorities set to enable this. To assess the open data maturity of European countries, Data.europa.eu, part of the European Commission, studied 35 countries:

- 27 EU member states,
- 3 European Free Trade Association (EFTA) countries (Iceland, Norway, Switzerland),
- 4 candidate countries (Albania, Montenegro, Serbia, Ukraine)
- 1 potential candidate country (Bosnia and Herzegovina).

The European Commission established four topline assessment criteria, which it then applied to every country in the study:²⁸

- **Policy:** this dimension sheds light on the open data policies and strategies in place in the European countries;
- **Impact:** this dimension analyzes the willingness, preparedness, and ability of European countries to measure both the reuse of and impact created by open data;
- **Portal:** this dimension focuses on the features, use and sustainability of countries' national open data portals;
- **Quality:** this dimension examines the measures adopted by portal managers to ensure the systematic harvesting of metadata from sources across the country.

Country overview

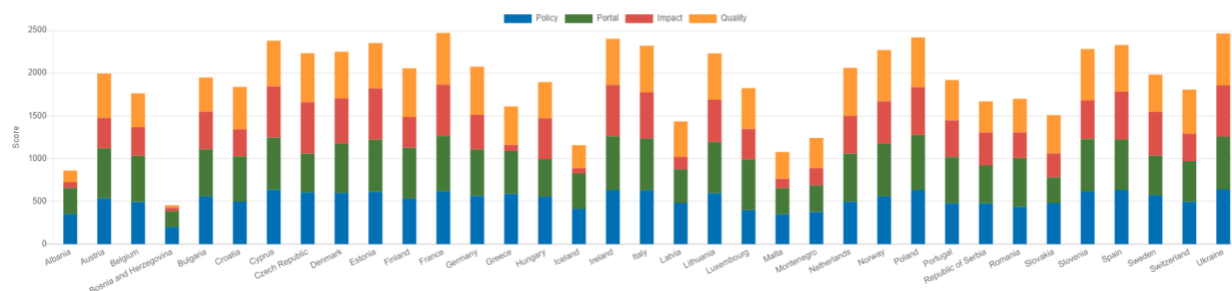


Figure 12: EU Country Overview

The four criteria areas of this measurement report serve as international guidelines for any country to determine its data maturity and transparency. It is important for the island of Curaçao to comply as it is a part of the Kingdom of the Netherlands and must, as one of the four countries of the Kingdom, develop its data maturity at a similar rate so as to comply within the EU and with other trade partners of the EU.

²⁷ <https://data.europa.eu/en/news-events/news/open-data-maturity-report-2022-out>

²⁸ <https://data.europa.eu/en/publications/open-data-maturity/2022#country-overview>

6.1 Concepts of data and data collection

Research has a wide scope and is applied in different businesses and industries for different purposes. Research is entirely based on information which is extracted from data. The term “data” originated from the singular word called “datum” which literally Datum means “something given”. Data is a collection of raw and unorganized facts that has no individual meaning. When raw data is processed, organized, and presented in a certain structure in such a way, that it becomes meaningful and useful, “Information”.

For example, during a census survey, various demographic data are collected such as name, age, occupation, education, income, etc., but only till it is analyzed and processed it will provide meaningful information like literacy rate, unemployment rate, average income, etc.

Primary and secondary data

Primary and secondary data sources are categories of data used in research and analysis, and they can be further categorized as internal or external data sources.²⁹ **Primary data** refers to original data that has been generated or collected directly from the source. It is data that is not previously published or processed by others. This could include sales records, customer feedback, or employee surveys.

Secondary data refers to data that has already been collected, processed, and published by someone else for a different purpose. Researchers or analysts use this data for their own investigations or studies. The table below highlights some difference between primary and secondary data.

Figure 13: Comparison of Primary and Secondary Data

Basis of Difference	Primary Data	Secondary Data
1) Meaning	The data collected at the source has not previously been published or processed by others.	When data, which was created earlier by some organizations for their own purposes, but is used in current research for a similar purpose, it is known as secondary data.
2) Cost	The collection of primary data is costly as it includes several tools and techniques.	It is less costly than primary data collection. The secondary data can be obtained easily, involving zero or very less amount of money. It is collected from some already available published or unpublished sources.
3) Sources	It is directly collected from respondents.	It is collected from some already available published or unpublished sources.
4) Methods	The methods used for primary data collection include interviews, questionnaires, observations and surveys.	The methods used for secondary data collection include studying and analyzing reports, journals, census, and different databases.
5) Reliability	Primary data should be more reliable as it has not been processed by others.	Secondary data is usually less reliable, as you don't have control over what methodology was used to collect the data. Secondary data often times is also filtered, cleaned and sometimes aggregated.

²⁹ <https://www.toppers4u.com/2022/07/primary-data-definition-features.html>

6) Scientific Method	The selection of primary data is scientific in nature. It includes forming hypothesis about the problem or situation, collecting data, and analyzing data to prove the hypothesis right or wrong.	The selection of secondary data is based on proximity to your own research questions. This can include the likeness of the data set, collection method, sample size and other variables important to your own query.
7) Precaution	Precautions are relatively nominal in collecting primary data than secondary data.	A lot of precaution is taken in the selection of secondary data.
8) Form of Data	Form of primary data is mostly raw which needs to be processed to get meaningful information. This may contain sensitive data.	Secondary data is already processed. It is usually depersonalized and filtered from anomalies.
9) Accuracy	Primary data is original and considered accurate at the time of collection. This includes any outliers and anomalies.	The secondary data is not completely accurate as it was developed for some other purpose.

By diversifying data sources and analyzing data from different channels, organizations can make more informed decisions and reduce potential biases that may arise from relying on a single source.

Internal and external Data

Companies may choose to segregate their data sources in internal data and external data. There are **advantages and disadvantages** in doing so.³⁰ Therefore, the importance of customization of approach is important. Following are important definitions and a list of considerations.

Internal data is data generated, collected or processed by the company itself as a means of supporting its core business. Is not restricted to but may include data from Customer Relationship Management (CRM) systems, Transactional Data, Employee Data, Product and Inventory Data etc.

One of the biggest **advantages** of internal data is that it is readily available for analysis. Another advantage of internal data is that it shows a very clear trajectory of your company and its processes. No outside body can explain your failures and successes as well as your internal data can. Your data will clearly show which departments are doing well and what can be done to improve them. In some cases, the lack of such data could show that there is a need to gather specific data as well, further enhancing the company’s capabilities.

A **disadvantage** from internal data is that your internal data may not be at its highest quality. ‘Bad data’ is what’s used to refer to data that refers to inaccurate information. Basing your decisions on inaccurate data will almost always lead to poor and devastating outcomes. Internal data is also guilty of not being able to provide all the necessary information. Sometimes you just have to make use of data from outside of your company, without which you will have voids in decision making.

It can also be costly to manage large amounts of internal data. If you’re trying to gather new customer insights through a different method, it might cost more in terms of time and money, than to just purchase the data from an external third-party source.

³⁰ <https://www.lido.app/post/internal-and-external-data>

External data is data generated, collected or processed by a third party, but used supplementary by the company to support business processes. Examples of external data are Market Research, Social Media Data, Economic Indicators and Census data.

An **advantage** of external data is that it gives business owners the ability to see how the world around them is functioning and make decisions accordingly. These may include quantitative as well as qualitative data.

Using external data also may relieve a company of the pressure of producing relevant data by itself. If existing databases contain enough value and suffice the core purposes, a company may opt to leverage external data. Generating data yourself can be a time-consuming and arduous process that is simply not worth the time.

A prevalent **disadvantage** in regards to external data is data discovery.

While data exists in extravagant amounts, finding relevant information can be difficult. It can take a long while to assess the credibility of any dataset you find and that's not going to be a cheap process. Apart from relevant information, you will also have to keep an eye out for misguided data. In today's world, fake news travels like wildfire, and coming across skewed statistics is not uncommon. Given how easy it can be to manipulate data, approaching it with caution cannot be overstated.

Companies often look at **internal and external data** separately due to several practical reasons and the distinct nature of these data sources. The four reasons are articulated here.

1. **Data Ownership and Access Control**

Internal Data: Organizations have direct ownership and control over their internal data. The data is typically readily available within the organization, which makes it easier to manage and analyze. Data security measures can be implemented as needed.

External Data: When it comes to for example third party data, companies may have limited control over data formats, updates, and access permissions. Access to external data may involve licenses or agreements with data providers, introducing complexities not present with internal data.

2. **Data Integration Challenges:**

Internal Data: Internal data is usually structured and stored within the organization's databases, making it relatively easier to integrate, analyze, and derive insights from. It can be readily combined with other internal data sources.

External Data: External data can come in various formats, including unstructured data from social media or market reports. Integrating external data into an organization's internal data ecosystem often requires additional data preprocessing and transformation, making it a more complex task.

3. **Data Quality and Consistency:**

Internal Data: The organizations can maintain high data quality standards for internal data, ensuring data consistency, accuracy, and reliability. This is possible when internally the right data collection processes and data governance practices are put in place.

External Data: The quality and consistency of external data can vary widely depending on the source. Companies may need to assess the reliability of external data providers and validate the data before use.

4. **Regulatory and Compliance Considerations:**

Internal Data: Companies must adhere to data protection regulations and compliance standards when handling internal data, particularly if the data contains sensitive customer or employee information.

External Data: Data providers may have their own terms and conditions, which companies must follow to remain compliant with legal and licensing requirements.

6.1 The 6 dimensions of data quality

Current trends in Artificial Intelligence (AI), Machine Learning (ML), and Big Data have been significantly impacted by data quality. AI and ML algorithms rely on large datasets to learn and make predictions. Therefore, the quality of the data used in training directly influences the accuracy and reliability of their outcomes.³¹ Big Data technologies enable the collection and storage of vast amounts of information, but ensuring data quality is critical to making meaningful insights from these datasets.

The old adage of computer programming – garbage in, garbage out – is just as applicable to today’s AI systems as it was to traditional software. Data quality means different things in different contexts, but, in general, good quality data is reliable, accurate and trustworthy.

Dimension is defined as a measurable feature of an object (ISO 9001). The object is in this context data. The term dimension is used to make the connection to dimensions in the measurement of physical objects (e.g., length, width, height). The term dimension in this context should not be confused with its use in the context of business intelligence where it refers to a category for summarizing or viewing data.

Data is a collective term for several concepts such as records, attributes, data values and metadata. Quality is defined as the degree to which inherent characteristics of an object meet requirements (ISO 9001). But we reformulate this definition as: the degree to which dimensions of a data concept meet requirements. The term ‘characteristic’ is replaced by ‘dimension’ because the latter term is more common in data land.

Quality is defined as the degree to which inherent characteristics of an object meet requirements (ISO 9001). But we reformulate this definition as: the degree to which dimensions of a data concept meet requirements.

Figure 14:

Six dimensions of Data Quality



³¹ Explain the 6 dimensions of Data Quality: <https://www.dama-nl.org/wp-content/uploads/2020/09/DDQ-Dimensions-of-Data-Quality-Research-Paper-version-1.2-d.d.-3-Sept-2020.pdf>

Further definitions of the six dimensions are as follows:³²

- **Accuracy:** Accuracy assesses the correctness and precision of data. Accurate data is free from errors, inconsistencies, and mistakes. It means that data values reflect the real-world entities they represent.
- **Completeness:** Completeness measures whether data is whole and comprehensive. It evaluates whether all the required data points are present. Missing or incomplete data can hinder analysis and decision-making.
- **Consistency:** Consistency examines the uniformity of data across different sources or within the same dataset. Consistent data follows the same standards, formats, and conventions.
- **Timeliness:** Timeliness focuses on whether data is up-to-date and relevant for the intended purpose. Timely data is available when needed and is reflective of the current state of affairs.
- **Relevance:** Relevance evaluates whether data is pertinent to the task at hand. Irrelevant data can clutter analyses and distract from the insights that are genuinely needed.
- **Integrity:** Data integrity concerns the overall trustworthiness of data. It checks for data's security and compliance with privacy regulations. Data with high integrity is protected from unauthorized access and maintains the privacy of sensitive information.

Data quality is essential for both internal and external data. Internally, it supports accurate decision-making, operational efficiency, and customer satisfaction while ensuring compliance and reducing costs. Externally, data quality is crucial for supporting market analysis, managing risks, gaining customer insights, and optimizing supply chains. Following the McKinsey think tank identifies key questions to ask.

A thorough evaluation of external data explores criteria in ten areas.

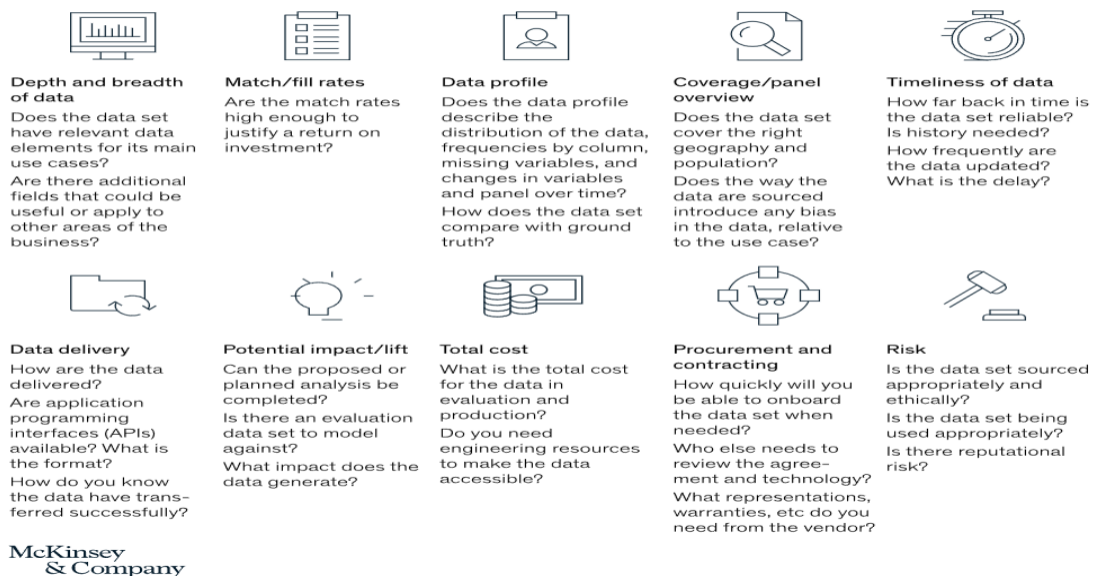


Figure 15

Data Definition Framework

Below is a visual framework that helps clarify types of business data.³³ This quadrant data framework is a way to think about a business's data in terms of the relation between Data source and Data Format.

³² Image and definitions: <https://www.ashineconsultancy.com/2021/04/30/establish-trust-in-your-data-with-master-data-management/>

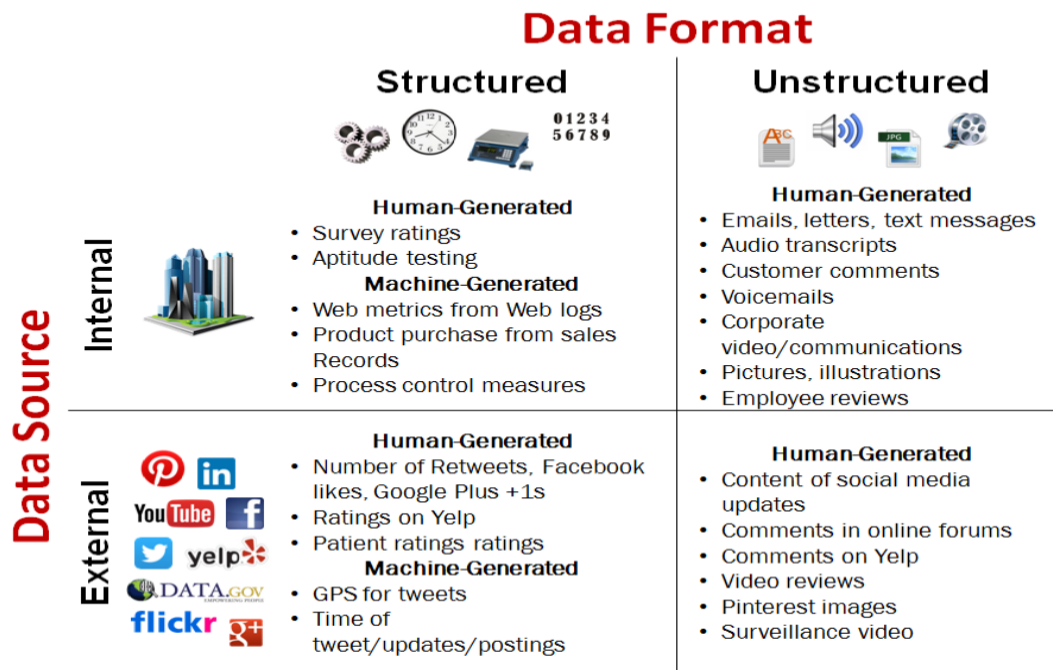
³³ <https://businessoverbroadway.com/2014/07/30/the-what-and-where-of-big-data-a-data-definition-framework/>

Using this framework, it can be seen that unstructured data can come from both internal sources and external sources.

Unstructured data is primarily human-generated. Human-generated data are those that are input by people. Structured data also can come from both inside and outside the business. Structured data includes both human-generated and machine-generated data. Machine-generated data are those that are calculated/collected automatically and without human intervention (e.g., metadata).

Due to the nature of the data the reliability will vary between quadrants. Structured / internal data might be more reliable and valid than unstructured / external data (e.g. customer sentiment metrics from social media content). As a result, the use of structured data might lead to a better understanding of a business' data.

Data Definition Framework




 Copyright 2014 Business Over Broadway

Figure 16 Data Format/Data Source Matrix

The listed examples in the matrix are not exclusive, but give an overview of well-known data sources and data formats.

Integrating and analyzing both internal and external data sources is crucial for making informed decisions and gaining a comprehensive understanding of an organization's landscape. When the actual data is unavailable, difficult to collect, or too costly to obtain, a related or substitute dataset (proxy data) can be used as an indirect way to infer or estimate the desired data.

Data by Proxy

Proxy Data are measurements that can be substituted for direct measurements when a direct measurement is not possible. In statistics, a proxy or proxy variable is a variable that is not in itself directly relevant, but that serves in place of an unobservable or immeasurable variable. In order for a variable to be a good proxy, it must have a close correlation, not necessarily linear, with the variable of interest.

Proxy data are not as reliable as direct data collection and can provide misleading results and, therefore, should not be used in the long term in the place of direct data collection. Because of the lack of reliable data in some sectors, a reliance on proxy data has formed. In order for the national data policy framework to work effectively, as much as possible direct data must be used across both the public and private sector. Various researches have shown that there are inherent biases in machine learning data by proxy and that extra measures must be taken to remove proxy discrimination in data-driven systems.³⁴

6.2 Grading Framework for data sources in Curaçao

By grading open data against these and other relevant criteria, users can assess the quality and usefulness of the data for their specific needs and purposes.

The list of elements to grade open data that is provided is not based on a specific global standard, but rather represents common best practices and criteria used in the open data community. There are several elements that can be used to grade open data, including:

- **Accessibility:** The data should be easily accessible to the public, without any barriers such as registration requirements or fees.
- **Machine-readability:** The data should be available in a machine-readable format that can be easily processed and analyzed by computers.
- **Structured vs unstructured:** Structured data is organized in a defined format, such as tables, while unstructured data does not have a predefined format. Structured data is generally easier to use and analyze.
- **Frequency of updates:** The data should be regularly updated to ensure its relevance and accuracy.
- **Downloadability:** The data should be downloadable in bulk, allowing users to access and analyze large amounts of data at once.
- **Data quality:** The data should be accurate, complete, and consistent.
- **Openness:** The data should be free to use, reuse, and redistribute without any restrictions or limitations.
- **Documentation:** The data should be accompanied by documentation that provides context and metadata, making it easier to understand and use.

³⁴ *Proxy Discrimination in Data-Driven Systems*, CMU, 25 July 2017, <https://arxiv.org/pdf/1707.08120.pdf>, *How Discrimination occurs in Data Analytics and Machine Learning: Proxy Variables*, Toward Data Science, 5 February 2020 (research summaries)

However, there are several global standards and frameworks that provide guidance on open data, such as the **Open Data Charter**, the **Open Data Institute's Data Ethics Canvas**, and the **various ISO standards for data quality**. These standards and frameworks may include similar or overlapping criteria for assessing open data, and can be useful for organizations or governments seeking to implement open data policies and practices.

Understanding the Overlaps and Nuances of Open Data Grading

When assessing the quality of open data, it's important to recognize that there are overlaps between the different criteria. While the 8 criteria for grading open data represent distinct concepts, there are instances where they may intersect or influence each other. However, it is crucial to emphasize that each criterion holds independent significance, contributing unique insights to the overall grading of Open Data.

Examples of Overlaps between Criteria

Machine-Readability and Structured Data: Structured data tends to be more machine-readable, as it is organized in a defined format that can be easily parsed and analyzed by computers. This is because the consistent structure of structured data facilitates machine processing and enables the identification of patterns and relationships.

Accessibility and Downloadability: Data that can be downloaded in bulk can significantly enhance its accessibility, allowing users to easily acquire and store large datasets for further analysis or manipulation. The ability to download data in bulk streamlines the data access process and enables users to work with the data in their preferred environment.

Data Quality and Frequency of Updates: Frequent updates contribute to improved data quality by ensuring that the information remains up-to-date and reflects the latest changes in the underlying data sources. The timely release of updated data ensures that users have access to the most accurate and relevant information for their analysis and decision-making.

Interpreting Each Criterion for Non-Technical Users

As the grading tool is intended for everyone to be able to assess how their data is presented, it is important that even non-technical users can understand the different criteria used. The following examples are given to make the definitions of each criterion easier to understand for non-technical users.

Accessibility: If data is like a library filled with knowledge, accessibility would be like having an open library door, inviting everyone inside without the need for a library card or any entry fees.

Machine-readability: For a human, a book is readable when suitable fonts, sizes and colors are used. For example, a book with a tiny font or with yellow color on a white background will be difficult to be read by a human. For machine readable data some formats are easier to process for a computer than others.

Structured vs Unstructured: Structured data is like a well-organized library, where the genres are grouped together and authors and titles are sorted alphabetically, making it easier to find and utilize information.

Frequency of Updates: For a news source to be relevant, it has to frequently update the news provided to the user. Similar to a continuously updated news feed, frequent updates ensure the data remains current.

Downloadability: A user can usually take a limited number of books from a library. If there is the option to take a whole bookshelf home, the user would have a wealth of information available at once.

Data Quality: Imagine data quality as the reliability of a well-researched and proofread document, ensuring it is accurate and trustworthy.

Openness: Some food and beverages have recipes that are known, but the original makers do not want others to modify the recipe. Openness would be sharing a recipe freely, allowing others to use and adapt it without limitations.

Documentation: This would be similar to an instruction manual, providing valuable information to comprehend and apply the data effectively.

Creating a Grading System for Open Data

As there is no standard or single procedure to grade open data, a grading system is proposed based on the elements presented above. This grading system is similar to a Likert scale, which is a widely used method for measuring attitudes, opinions, and perceptions. It consists of a series of statements or questions to which respondents can indicate their level of agreement or disagreement. A Likert scale typically uses a fixed set of response options (e.g., strongly agree, agree, neutral, disagree, strongly disagree) that is then transformed using a numerical scale, ranging from 1 to 5. For the grading system, a similar approach is used with a numerical range for each of the elements, where 1 is a worst-case scenario for the criteria and 5 is a best-case scenario. For example, for “Machine Readability” a 1 would be “Data is provided in a non-machine-readable format like a scanned image or PDF” and 5 would be “Data is provided in machine-readable formats, follows standard data structures, and includes links to other data sources”. The grading system for open data criteria can be considered a structured evaluation framework rather than a traditional Likert scale. This framework allows for the systematic assessment of open data based on predefined criteria, enabling organizations to evaluate and improve their open data practices.

Potential Biases

One potential bias that can arise when using the grading system is the aversion to using the extremes (1 and 5). Individuals may hesitate to assign the lowest or highest grades, preferring to use the middle options, which could lead to an overall rating that is higher than it should be. To mitigate this bias, it is important to clearly define the meaning of each grade and to ensure that the evaluators are comfortable and confident in using the entire scale.

Benefits of the Grading System

Despite this potential bias, the grading system provides a structured and consistent approach to evaluating open data. The clear definitions of each grade and the range of options allow for a more comprehensive assessment of the open data collection, highlighting both strengths and areas for improvement. This information can be used to identify areas of focus for improvement, track progress over time, and inform decision-making regarding open data initiatives.

Methodology of research on Openness of Data on Curaçao.

The Think To Do Institute conducted research on the “openness of data” of several entities in Curaçao, using the designed grading tool. Many of these entities are listed on the Curaçao Data Driven DataWiki. This wiki is intended to be used like the yellow pages as a means of indexing locally available resources. Curaçao Data Driven is a non-profit platform for creating awareness and sharing knowledge to create a culture that uses data to make better decisions.

The entities chosen for this research were those that presented data on their public websites. At least five datasets or documents were downloaded from each site to evaluate the criteria for data openness.

The criteria for assessing data openness were divided into two categories. First, criteria like Accessibility, Machine-readability, Structured vs Unstructured, Downloadable, Documentation, and Openness were considered more straight-forward to assess. Second, criteria like Frequency of Updates and Data Quality were considered more complex.

For the Frequency of Updates, the research team examined the historical data presented on the websites. The frequency of updates was determined based on this review. For instance, entities publishing annual reports were evaluated based on the most recent report available at the time of the assessment. The presence of notable gaps in the data was also assessed to grade the frequency of updates.

Assessing Data Quality proved more challenging as the researchers did not always possess specific domain knowledge to verify the accuracy of the presented data. However, as data specialists, they used their expertise to identify indicators within reviews, documentation, and data presentation that offered insights into data quality.

Results of Sampling of Openness of Data on Curaçao

In terms of accessibility, the majority of the data was readily available on the public websites without any need for registration. In some instances, there were additional benefits associated with registration, but none of the cases necessitated payment. This high accessibility score reflects the ease with which the data can be accessed by the public.

When it comes to machine-readability, most of the lower scores were attributed to information being presented in images, scanned PDFs, and similar formats that require additional processing. In most of those cases the data is also not very well structured, which also lowers the score for structured data.

In terms of downloadability, none of the sites assessed in the research offered bulk downloads for their data. Most data are presented as single file downloads, which means that while the data can be downloaded, it may not be feasible for users who wish to access large amounts of data at once.

Regarding openness, there were no explicit licenses or indications on the sites that the data could not be re-used. As a result, it was assumed that the data is open, but it was considered to have restrictions until a clear notice was posted on the sites with explicit information about the terms of use for the data.

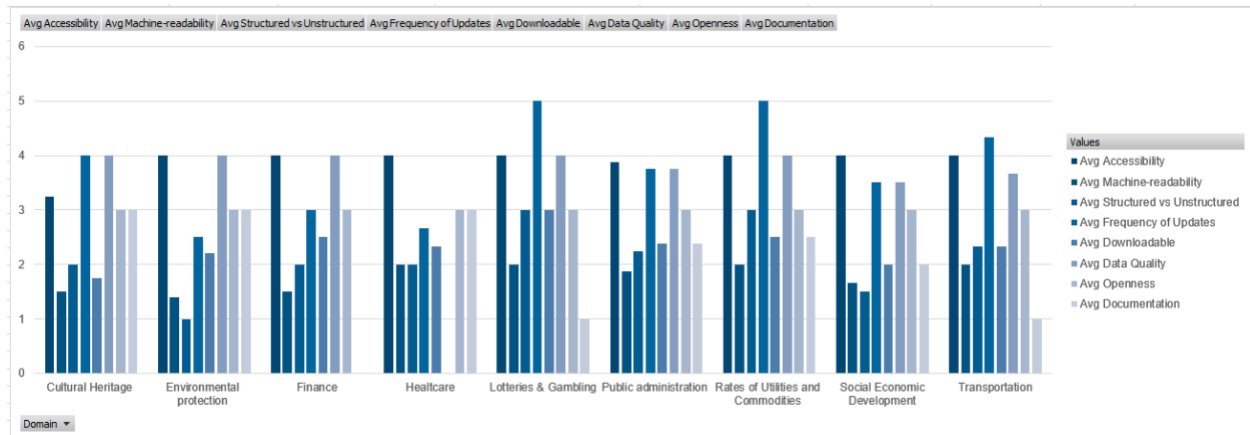
Most of the data available don't have clear documentation, but in most cases the data is self-explanatory and does not require much documentation. In some of presented data from formal researches, the documentation presented for the data is acceptable, with room for improvement.

It's important to note that the grades presented do not provide a comprehensive picture of the openness of data on Curaçao. The research was limited to entities with data on public sites, which means that many entities, particularly those without public data, were not considered. If the grades were averaged across all entities on Curaçao, the majority would likely score zero, significantly skewing the average.

Furthermore, it's crucial that the grading tool is accessible to everyone, allowing domain experts to assess Data Quality and know what to look for. This ensures a more accurate and comprehensive evaluation of data openness on Curaçao.³⁵

Figure 17: Results of Curaçao Openness of Data

Row Labels	Values							
	Avg Accessibility	Avg Machine-readability	Avg Structured vs Unstructured	Avg Frequency of Updates	Avg Downloadable	Avg Data Quality	Avg Openness	Avg Documentation
Cultural Heritage	3.25	1.5	2	4	1.75	4	3	3
Environmental protection	4.00	1.40	1.00	2.50	2.20	4.00	3.00	3.00
Finance	4.00	1.50	2.00	3.00	2.50	4.00	3.00	3.00
Healthcare	4.00	2.00	2.00	2.67	2.33	3.00	3.00	3.00
Lotteries & Gambling	4.00	2.00	3.00	5.00	3.00	4.00	3.00	1.00
Public administration	3.88	1.88	2.25	3.75	2.38	3.75	3.00	2.38
Rates of Utilities and Commodities	4.00	2.00	3.00	5.00	2.50	4.00	3.00	2.50
Social Economic Development	4.00	1.67	1.50	3.50	2.00	3.50	3.00	2.00
Transportation	4.00	2.00	2.33	4.33	2.33	3.67	3.00	1.00
Grand Total	3.88	1.75	2.21	3.75	2.28	3.82	3.00	2.16



6.3 ISO standards for data

Introduction to ISO High Structure (HS) previously known as High Structure level (HSL):

In today's rapidly evolving global landscape, organizations across various sectors are continually seeking ways to enhance their operational efficiency, ensure consistent quality, and maintain robust information security practices. Achieving these objectives requires a systematic and standardized approach, which is where the *International Organization for Standardization (ISO)* steps in.

One of the prominent frameworks introduced by ISO is the *High Structure Level (HSL)*. The ISO High Structure Level (HSL) represents a set of international standards meticulously designed to guide organizations toward excellence in their management systems. These standards provide a

³⁵ *Sampling of Openness of Data on Curaçao*, Think To DO Institute, Curaçao, 2024.

comprehensive framework for organizations to establish, implement, maintain, and continually improve their processes, ensuring they meet stringent criteria for quality, efficiency, and security.

The HSL framework encompasses a range of key elements, including strategic planning, risk management, leadership, resource optimization, and performance evaluation, among others. Organizations that adhere to the *ISO High Structure Level* not only enhance their internal processes but also gain a competitive edge in the global marketplace. Compliance with HSL standards demonstrates a commitment to quality, reliability, and partners, and consumers and clients.

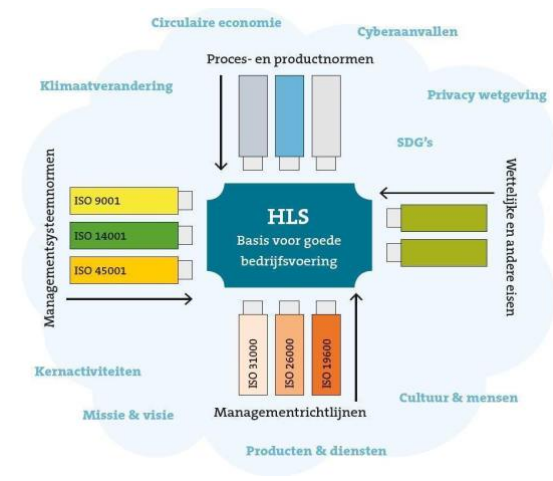


Figure 18: HSL Framework

This introduction to ISO High Structure Level explores the fundamental principles, benefits, and significance of adopting this framework, providing a valuable foundation for organizations striving for excellence in their operations. ³⁶

ISO standards play a crucial role in various aspects of data management, including data creation, processing, storage, usage, archiving, and destruction. For instance, ISO standards ensure that data is created in a structured and consistent manner, facilitating easy interpretation and analysis. Standardized data creation processes help organizations maintain data accuracy, completeness, and relevance, ensuring reliable information for decision-making. ISO Standards can also provide guidelines for secure and efficient data processing and storage methods. Adhering to these standards ensures that data is processed accurately, protecting it from errors and unauthorized access. The ISO standards have various numbers assigned indicating the focus of the standards. (See Appendix for further definitions) Standardized storage practices help organizations optimize their storage systems, ensuring data availability and integrity. (reference to ISO 8000 and ISO 27000 series). Implementing these standards promotes and define protocols for responsible data usage, ensuring that data is used ethically and legally. Compliance with these standards protects individuals' privacy rights and prevents misuse of sensitive information. (Reference: ISO 27701 and ISO 29100)

Organizations following ISO guidelines build trust with customers, stakeholders, and regulatory bodies, enhancing their reputation. For systematic data archiving, ensuring that valuable information is preserved for legal or historical purposes, organizations can leverage these best practices such as ISO guidelines 11506:2017 for document management applications.

Archiving standards help organizations establish organized and secure archives, making it easier to retrieve data when needed. Properly archived data can support audits, investigations, and research, enhancing the organization's credibility. ISO 27001 standards outline secure methods for data destruction, preventing unauthorized access to discarded or obsolete information. Adherence to these standards protects against data breaches and identity theft, safeguarding both individuals and organizations.

³⁶ <https://www.nen.nl/en/managementsystemen/high-level-structure-hls>

Proper data destruction practices also ensure compliance with data protection regulations and industry standards. In summary, ISO standards provide a structured framework for managing data throughout its lifecycle. By following these standards, organizations can enhance data quality, security, and compliance. This, in turn, fosters trust, reduces risks, and promotes responsible data management practices, benefiting both the organization and the individuals whose data is being handled.

Importance of a Global Data Protection Program

In our interconnected world, where data flows seamlessly across borders and digital interactions are ubiquitous, ensuring the privacy and security of personal information has become a paramount concern for individuals, organizations, and governments alike. With the advent of advanced technologies, the significance of safeguarding sensitive data on a global scale cannot be overstated. This urgency has given rise to the concept of a Global Data Protection Program, a strategic and comprehensive approach employed by organizations to manage and protect personal data across international boundaries. A Global Data Protection Program is more than just a set of policies and procedures; it represents a commitment to respecting individuals' privacy rights regardless of their location. Such a program encompasses a holistic framework that addresses legal compliance, ethical considerations, and customer trust. It not only safeguards sensitive information but also fosters transparency, accountability, and responsible data handling practices within an organization. The importance of a Global Data Program lies in its ability to navigate the complex web of international data protection laws and regulations.

With stringent legislation such as the **General Data Protection Regulation (GDPR)** in the European Union, **California Consumer Privacy Act (CCPA)** in the United States, **Brazilian General Data Protection Law (LGPD)** and more, organizations operating globally must adhere to a patchwork of rules. A well-designed Data Protection Program ensures that an organization complies with these regulations, avoiding legal pitfalls, hefty fines, and damage to its reputation. Moreover, in an era where data breaches and cyber threats are prevalent, a robust Global Data Protection Program serves as a shield against unauthorized access, identity theft, and financial fraud. It builds customer confidence by demonstrating a commitment to data security, thereby preserving the organization's reputation and customer loyalty. (Reference ISACA 2022 digital trust report).

Beyond legal and security aspects, a Global Privacy Program is essential for fostering innovation and collaboration. By instilling a culture of privacy-consciousness, organizations can freely explore new technologies and business opportunities, knowing that they have a solid foundation of privacy protections in place. This approach encourages responsible data sharing, enabling collaboration with international partners, suppliers, and customers without compromising the integrity and confidentiality of personal information.

Leveraging ISO Harmonized Structure for Building a Robust Global Data Protection Program

The *ISO Harmonized Structure (HS)*, common to all ISO management system standards, offers a unified framework that streamlines the process of developing a global data protection program. By aligning with this structure, organizations can integrate their data protection initiatives seamlessly with other management systems, such as quality management (ISO 9001), information security management (ISO 27001) and information privacy management (ISO 27701). Utilizing the ISO HS enables organizations to identify, assess, and manage data protection risks systematically. (reference iso 31000 risk guidance) By following the structured approach outlined in the ISO standards, organizations can establish robust risk management processes that are consistent across all their operations, ensuring a comprehensive understanding of potential data protection threats. The ISO (HS) incorporates legal and regulatory

requirements, providing a foundation for organizations to align their local, regional and global data protection program with international laws such as the General Data Protection Regulation (GDPR) in the European Union.

Compliance with these regulations is crucial for organizations operating across borders, and the ISO HS acts as a guide to meeting these complex legal obligations. Building a global data protection program based on the *ISO Harmonized Structure* demonstrates an organization's commitment to transparency and accountability. Stakeholders, including customers, partners, and regulatory bodies, are more likely to trust organizations that adhere to internationally recognized standards. This trust is essential for fostering strong relationships and maintaining a positive reputation on a global scale.

One of the core principles of the *ISO Harmonized Structure* is continuous improvement. By embedding this principle into the global data protection program, organizations can establish a culture of constant vigilance, ensuring that data protection measures are always evolving to address emerging threats and challenges effectively. In addition, the harmonized approach streamlines resource utilization by eliminating redundant processes and optimizing efforts. This efficiency allows organizations to allocate resources effectively, enhancing the implementation and maintenance of their global data protection program without unnecessary complexity.

6.4 Methodology of choice

The most usable of the three sets of guidelines seems to be the *Open Data Charter*. Because this Charter is a global initiative that seeks to promote the adoption of open data policies and practices by governments and organizations worldwide and consists of the six principles that outline the key characteristics of open data, it provides the most generic approach.

Its set of implementation guidelines provides practical advice on how to implement open data policies and practices. These guidelines cover different aspects that even the novice framework developer can understand and follow in the areas of the open data lifecycle, including planning and prioritization; data publication; data management; data use; and impact measurement. Overall, the *Open Data Charter* aims to promote a global culture of open data that supports sustainable development, innovation, and democratic governance which is the goal of a framework that works for both the public and private sectors.

6.5 Best practices for managing and making data publicly available

Managing Data Responsibly

As companies become ever more data-driven, the issue of availability becomes ever more important. Factors such as storage, backup, recovery, security, and network performance can affect data availability.

The biggest obstacle is ensuring the design of the infrastructure for long-term, uninterrupted availability. This requires focus on the infrastructure to ensure that the data is redundant – or, in other words, that there are multiple sources of the data available. This safeguards that a failure in one of the disks, servers or databases that hosts the data will not lead to a disruption in availability.

The multiple sources build redundancy and backups into the data infrastructure, and enable them via “automated failover”. Automated failover means (as the term implies) that the backup system takes over automatically when the main system goes down.

Another best practice related to infrastructure is “Infrastructure overload” prevention. The best defense against this risk is to build scalability into the national data infrastructure. This practice means that from the highest level of oversight of the system that scalability is seen from the big-picture perspective while ensuring that new infrastructure can be set up quickly when it is needed. This requires long-term vision and structural design priorities from the outset.

Giving priority attention to the infrastructure makes the other factors related to storage, backup, recovery, security and network performance easier to manage.

Making Data Publicly Available

Multiple countries have examples of Fair Principles for Data. In order to follow these other countries, each country needs to approve and comply with these Fairness Principles for Data. The core principles are that data is: Findable, Accessible, Interoperable, Reusable.³⁷

These principles are foundational in ensuring that data is collected and analyzed in an ethical and transparent manner, and that the data is treating all individuals in the dataset equally and without bias. When each entity then becomes a part of the national data framework following these principles, then the entire system can be assured that the data that is exchanged between local entities and across public and private data networks will be compliant with availability standards.

³⁷ “How to Make Your Data Fair”, Force11, Utrecht University, 2016.

7 The industry practice for the use of data within mass media communication

There is a difference between “being trustworthy” and “being trusted,” according to a report published in 2020 by the Open Data Institute - because being trusted relies on a third-party assessment. Many companies have been publishing their own principles and values when it comes to designing and deploying emerging technologies (Google, for example, started publishing AI principles in 2018 that include ‘Be accountable to people.’)

But principles are only useful if they are implemented. To do so effectively, values and principles need to be considered throughout the data lifecycle, and communicated effectively both externally and internally. The data policies, practices and frameworks commonly used by modern organizations generally seek to incentivize good practices on collection, use, and sharing.³⁸

7.1 Types of mass media communication

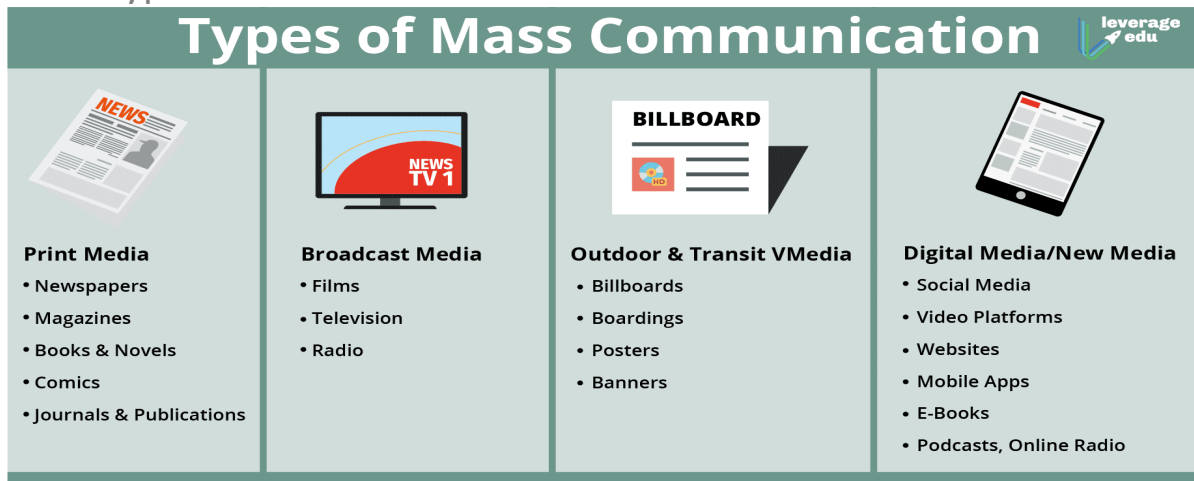


Figure 19: Types of Mass Communication Leverage.edu 2022

Some of the different types of mass media communication are presented here:

- Traditional media: Traditional media includes traditional advertising and marketing methods that businesses have relied upon for years, such as television, radio, and print advertisements.
- Print media: Print media includes newspapers, magazines, books, and other printed materials.
- Broadcast media: Broadcast media includes information transmitted through one of several mass communication channels, such as television and radio.
- Digital media: Digital media includes digital advertising and marketing methods that occur online or involve the internet, such as social media or email marketing.
- Social media: Social media platforms allow users to create, share, and interact with content. Examples include Facebook, Instagram, Twitter, and TikTok.
- Podcasts: Podcasts are digital audio files that can be downloaded and listened to on a variety of devices.

³⁸ Data Policy Insight Briefing, World Economic Forum: 2022.

The use of mass media communication has evolved over time, with newer forms of media such as social media and podcasts becoming more and more popular. Understanding the different types of mass media communication is important for businesses and organizations that want to effectively communicate with their target audience. By using a combination of traditional and the newer forms of digital media, businesses and organizations can reach a wider audience and target specific groups of people. They should also consider their target audience when choosing mass media channels to use. By understanding the demographics and preferences of their target audience, businesses can select the most effective channels to reach and engage with them.

7.2 What are Social Media and Influencers

Social media can be defined as a group of internet-based applications that facilitate the creation and sharing of content. It has transformed the way we communicate, interact and access information. Social media influencers are individuals who have gained a reputation for their knowledge and expertise on a specific topic. They generate large followings of engaged people who pay close attention to their views and can be one who can persuade others by virtue of their authenticity and reach. Different types of influencers exist in social media. They can be classified based on the number of followers they have, from "nano influencers" with 1,000-10,000 followers up to "celebrities" with a million or more followers. They can also be classified based on their brand affinity, which is the amount of affinity and commitment to a given brand.

There are also different categories of influencers³⁹:

- **Celebrity influencers:** These are the most well-known influencers, as they have acquired their following from their celebrity status.
- **Consumer influencers:** These are everyday people that have gained a following due to their personality and relatability.
- **Micro influencers:** Also known as expert influencers, these are everyday people that have gained a following and topical authority due to their knowledge in a specific area.
- **Content creators:** These include professional bloggers, vloggers, and photographers. Their role includes developing new content that readers are interested in keeping up with regularly.

The impact and reach of social media and influencers have increased significantly over time. Influencers have the ability to create trends and encourage their followers to buy products they promote. Brands often find significant value in influencers because they can reach great size of target audiences that match the brand's preferred customer base.

It is important to make the distinction between social media marketers and social media influencers, that are two different roles in the digital marketing industry. A social media marketer is a professional who uses social media platforms to promote a product, service, or brand. They create and manage marketing campaigns, analyze their performance, and adjust strategies based on these analyses. Their goal is to increase brand awareness, generate leads, and ultimately drive sales. They may work as part of a marketing team in a company or as independent consultants or agencies.

On the other hand, a social media influencer is an individual who has built a reputation for their knowledge and expertise on a specific topic. They have a dedicated social following and are seen as experts within their niche. Influencers create original content and engage with their followers regularly,

³⁹<https://engaiodigital.com/types-of-influencers/>

which allows them to influence their followers' purchasing decisions due to their authority, knowledge, or relationship with their audience.

Businesses of all sizes and across industries use social media influencers to promote their products or services. This includes sectors like fashion, beauty, fitness, travel, food, and technology, among others. Non-profit organizations and government agencies also use influencers to raise awareness about causes or campaigns.

7.3 Reach, Resonance and Relevance

The **3R's of Influencers - Reach, Resonance, and Relevance** - are essential components of influencer marketing. The 3R concept has been widely accepted by marketers and researchers as a set of criteria for selecting the ideal influencer for a brand. Each R represents a different aspect of an influencer that, when combined, makes for the ideal partner for a brand.⁴⁰ The following is a brief explanation of each R:

1. **Reach** refers to the size of an influencer's audience and the potential number of people who can be reached through their content. It is one of the most important factors to consider when choosing an influencer. A brand may choose to work with a celebrity influencer with millions of followers to get a significant initial boost.
2. **Resonance** measures the level of engagement and impact an influencer has on their audience. It is about how well an influencer's content resonates with their followers and how much influence they have over their audience. An influencer who consistently receives high engagement rates on their posts is likely to have strong resonance with their audience.
3. **Relevance** assesses whether the brand promoter and their target market are a suitable fit. It simply signifies the alignment between an influencer's content and the brand identity, niche, or product. A brand that sells fitness products may choose to work with a fitness influencer who shares similar values and promotes a healthy lifestyle.

In publications about influencer marketing, resonance and relevance are less talked about than reach in publications.

- Reach can be measured by the number of followers an influencer has on social media or the number of views their videos get on YouTube. Resonance and relevance, on the other hand, are more difficult to measure.
- Reach is something that can be easily seen on an influencer's profile page. Resonance and relevance, on the other hand, are more subjective and require more effort to assess.
- Some brands, such as consumer packaged goods brands, are more concerned with reaching a large audience than they are with building relationships with a smaller, more engaged audience.

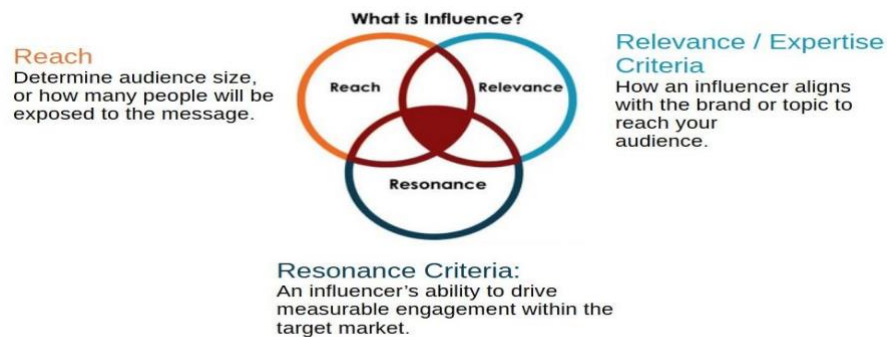


Figure 20: 3Rs: essential components of influencer marketing.

⁴⁰ <https://www.bridgingpointsmmedia.com/services/influencer-marketing>

There are documented cases where social media platforms have inflated views of content to let the influencer think they had greater reach than they really have. In 2018, Facebook was accused of knowingly inflating its video metrics for over a year, leading many media organizations to put an emphasis on Facebook video and chase views to the detriment of other editorial efforts. This suggests that social media platforms may inflate views to attract more ad spend or to gain recognition. It is important for brands and influencers to be aware of these issues and to take steps to ensure that their metrics are accurate and reliable.

The influencer has a dashboard with data provided by the social media platform, including for example location of viewer or demographics. This data is typically not publicly available, but it can be shared with third-party companies that want to have a partnership with the influencer. Why is this important?

The company that wants to hire an influencer has to base the decision on data provided by the influencer and the social media platform. When estimating the reach and resonance of an influencer, the company should consider the following factors:

- The percentage of an influencer's followers who actively interact with their content, such as liking, commenting, or sharing. A high engagement rate indicates a more resonant and relevant audience.
- Look for meaningful interactions, such as thoughtful comments or discussions, rather than just a high number of generic likes or emojis. This can help assess the level of resonance and relevance of the influencer's content.
- Evaluate the influencer's posting frequency and regularity. A consistent content schedule can help maintain audience interest and improve reach and resonance over time.
- While a third-party observer may not have access to detailed demographic information, they can still get a sense of the influencer's audience by analyzing the content, comments, and engagement. Look for alignment between the influencer's target audience and the third-party's marketing goals.
- Consider whether the influencer's content, values, and messaging align with the third-party's brand identity and target audience. A strong brand alignment can enhance the influencer's resonance and relevance for the third-party's marketing efforts.
- Building a long-term relationship with an influencer can help establish trust and authenticity with their audience, leading to better reach and resonance over time. Look for influencers who have a track record of successful partnerships and collaborations.

7.4 Integrity, accountability, in data from mass media

Integrity and accountability are essential components of data governance and are quite important in the context of mass media communication. Mass media plays an important role in our society by keeping us informed about current events and shaping our understanding of the world. However, it is important to be critical of the information we consume from mass media, as it is not always accurate or unbiased. Both organizations (producers of mass media) and users (of said media) have a responsibility in checking for the integrity of mass media data and holding organizations accountable.

Organizations presenting data in mass media should take the following into account:

- Quality of the data: carefully evaluate the quality of the data they are using. This includes assessing the source of the data, the data collection methods, and the potential for bias.

- Context of the data: present data in a way that provides context and understanding. This includes explaining the significance of the data, how it relates to other relevant information, and any potential limitations of the data.
- Potential for bias: be aware of the potential for bias in their data collection and analysis methods. They should take steps to mitigate bias and be transparent about any potential biases in their reporting.
- Impact of their reporting: consider the potential impact of their reporting on the people and communities involved. They should be mindful of the potential for harm and take steps to minimize any negative impacts.

Users of mass media have a responsibility to check for data integrity in the presented information and hold the organizations accountable:

- Consider the source: Is the source of the data reputable and credible? Do they have a track record of accurate and unbiased reporting?
- Look for multiple sources: Does the information presented in the report match up with information from other reputable sources?
- Be skeptical of headlines: Headlines can often be misleading or sensationalized, so it is advised to read the full article before forming an opinion.
- Be aware of own biases: Everyone has biases that can influence how information is interpreted, so the user should try to be objective when evaluating mass media reporting.
- Hold journalists and organizations accountable: If the user sees something that they believe is inaccurate or misleading, they should contact the journalist or organization and let them know. They can also share their feedback on social media or with other people they know.

7.5 The effects of information and disinformation on public opinion

Public opinion is important to democracy because it encourages elected officials to act in the best interest of their voters if they want to be re-elected.

Disinformation threatens freedom of thought, the right to privacy and the right to democratic participation, as well as endangering a range of economic and social structures. Propaganda, misinformation and fake news have the potential to polarize public opinion, to promote violent extremism and hate speech and, ultimately, to undermine democracies and reduce trust in the democratic processes. Disinformation erodes the public's confidence in government policies, processes and outputs.

The role of the media is to effectively discriminate information so that the public can form opinions for themselves. The following four roles are identified for all media types: Media as transparency watchdog, Media as a campaign platform, Media as an open forum for debate and discussion/public voice, Media as public educator. Transparency is required on many levels including for access to information; accountability and legitimacy of individuals, institutions and processes themselves; and for rightful participation and public debate.

Free press is under threat or declining precisely because it is so important to democracy. Democracy research has confirmed that authoritarian governments want to retain power above all else. When there is no free press, when the stream of information is controlled by the government or oligarchs, the people are given a distorted picture of what's happening.⁴¹ This is important because the media landscape has changed. Media platforms such as Facebook, Google and other Big Tech companies aggregate news and share it with their users, with little to no revenue flowing back to the source. This regime must change if we are to protect the plurality and diversity of our media landscape and maintain a truly free press.⁴²

Media bias in social media is also reflected in hostile media effect. Social media has a place in disseminating news in modern society, where viewers are exposed to other people's comments while reading news articles. Media bias is also reflected in search systems in social media. Juhi Kulshrestha and her research team found through research in 2018 that the top-ranked results returned by these search engines can influence users' perceptions when they conduct searches for events or people, which is particularly reflected in political bias and polarizing topics.⁴³

Because the access to information is quickly turning toward social media, this bias and its effect on disinformation through influencers is important to recognize and protect against.

⁴¹ 2023 World Press Freedom Index-journalism threatened by fake content industry, Reporters Without Borders(RSF), 2023.

⁴² Ibid.

⁴³ Kulshrestha, Juhi; Eslami, Motahhare; Messias, Johnnatan; Zafar, Muhammad Bilal; Ghosh, Saptarshi; Gummati, Krishna P.; Karahalios, Karrie (2019). "[Search bias quantification: investigating political bias in social media and web search](#)" (PDF). *Information Retrieval Journal* (2019) 22:188–227. **22** (1–2): 188–227. doi:[10.1007/s10791-018-9341-2](#). S2CID 52059050

8 Ethical Boundaries and Concerns

Creating a national data framework demands careful consideration of ethical boundaries and concerns to protect privacy, ensure data security, promote fairness, and maintain public trust. By addressing these concerns, governments can establish robust safeguarding measures and guardrails to navigate the complex ethical landscape surrounding data frameworks.

It is important to note that integrity is a cornerstone of a system of sound public governance. It assures citizens that the government is working in their interest, not just for the select few, and is vital for the economic prosperity and well-being of society as a whole.

8.1 Safeguarding and Guardrails

There must be included in the safeguards and guardrails of the national data framework, rules and consequences for conflict of interest, nepotism and cronyism with guidelines for whistleblowers to call out violations. This creates and actualizes the ethical boundaries that are critical to the successful implementation of the national data policy framework.

Following are some key considerations with regards to safeguarding and establishing necessary guardrails:

1. **Privacy Protection:** One of the most significant ethical concerns is the protection of individuals' privacy. National data frameworks should ensure that personal data is collected, stored, and used in compliance with relevant privacy laws and regulations. Strong safeguards should be in place to prevent unauthorized access, use, or disclosure of personal information.
2. **Informed Consent:** Individuals should have the right to be informed about the collection and use of their data and provide explicit consent for its inclusion in the national data framework. Transparent policies and procedures should be in place to obtain informed consent, ensuring that individuals understand the purpose and potential implications of sharing their data.
3. **Data Security:** Safeguarding the data within the national framework is crucial. Adequate security measures, including encryption, access controls, and regular monitoring, should be implemented to protect against data breaches, hacking, or unauthorized access. Regular audits and assessments of data security practices should be conducted to identify and address vulnerabilities.
4. **Data Quality and Accuracy:** It is essential to ensure the accuracy, reliability, and relevance of the data collected within the national framework. Rigorous data quality controls, including validation processes, should be in place to minimize errors, inconsistencies, or bias that could negatively impact decision-making based on the data.
5. **Anonymization and De-identification:** To mitigate privacy risks, personal data should be appropriately anonymized or de-identified before its inclusion in the national framework. This process involves removing or encrypting personally identifiable information to prevent the re-identification of individuals.
6. **Data Governance and Accountability:** Clear governance structures and accountability mechanisms should be established to oversee the national data framework. This includes defining roles and responsibilities, establishing standards and guidelines, and implementing mechanisms for auditing and redress in case of misuse or breaches.
7. **Equity and Fairness:** National data frameworks should be designed and implemented in a manner that ensures fairness and avoids perpetuating biases or discrimination. Steps should be taken to identify

and address potential biases in data collection, analysis, and decision-making processes to ensure equitable outcomes.

8. **Transparent and Open Access:** There should be transparency around the purposes and use of the national data framework. Considerations should be given to enable appropriate access to the data by authorized users, researchers, and policymakers while ensuring adequate protections to prevent misuse or unauthorized access.

9. **Public Engagement and Consultation:** The development and implementation of national data frameworks should involve public engagement and consultation to ensure that diverse perspectives and concerns are considered. This can help build trust and legitimacy and reduce the potential for unintended negative consequences.

10. **Ethical Review and Oversight:** Independent ethical review boards or committees can play a crucial role in assessing the potential ethical violations of the national data framework and providing guidance on its development, operation and consequences for non-compliance.

As such international frameworks influence each country to implement and comply within the expected ethical boundaries of those frameworks, it is imperative that at the local level a national integrity system be adopted. The lack of such a system for Curaçao, including policies that address emerging technologies, weakens the ability of institutions to perform the tasks they are designed to do for the country, consequently weakening the economic and social systems necessary for the country to thrive. The National Integrity System (NIS) should be treated as an “urgency law” as it affects every other law’s integrity and implement ability.

9 Working across international data frameworks (GDPR, CCPA, PDPA(Asia/Singapore))

When working across international data frameworks such as the **General Data Protection Regulation (GDPR)**, the **California Consumer Privacy Act (CCPA)**, and the **Personal Data Protection Act (PDPA)** in Asia/Singapore, there are several considerations.

It is important to note that these are general considerations, and that specific steps and strategies may vary depending on the individual countries and their legal, cultural, and political contexts.

Even when there are data protection authorities, the institutions responsible for interpreting and enforcing data protection laws in most countries often lack functional independence from the executive branch or other ministries, particularly in lower income countries, which makes it difficult for them to resist political influence or to hold other government actors accountable (Davis, 2021). There also are wide disparities in the level of human and financial resources available to data protection authorities across regions and economic classification.⁴⁴

When a county does not have a data policy framework in place to comply with regulations such as the **General Data Protection Regulation (GDPR)** or the **California Consumer Privacy Act (CCPA)**, there are several steps that can be taken to address the situation. Here are some actions that can be considered. These are not presented in any priority order but do follow a logical sequence.

1. **Assess the current data practices:** Conduct a thorough review of the county's data handling processes, including data collection, storage, processing, and sharing. Identify areas where the county may be collecting or using personal data that could fall under the scope of GDPR or CCPA.
2. **Seek legal expertise:** Consult with legal experts who specialize in data protection and privacy laws. They can provide guidance on the specific requirements of GDPR or CCPA and how they may apply to the county's operations.
3. **Educate and train employees:** Provide training to employees on data protection principles, privacy practices, and their responsibilities in handling personal data. Raise awareness about the importance of complying with GDPR or CCPA regulations and the potential consequences of non-compliance.
4. **Review third-party agreements:** Assess existing agreements with third-party service providers and vendors to ensure they comply with GDPR or CCPA requirements. Update contracts or seek legal advice to ensure that data processing activities conducted on behalf of the county are carried out in compliance with the relevant regulations.
5. **Implement necessary safeguards:** Identify and implement appropriate technical and organizational measures to ensure data protection. This may include implementing data security protocols, access controls, encryption, and anonymization techniques.
6. **Establish data subject rights processes:** Define procedures for handling data subject rights requests, such as access, rectification, erasure, and data portability. Ensure that mechanisms are in place to promptly respond to such requests and address data subjects' rights effectively.

⁴⁴ The Ultimate OSINT Handbook: A Guide to Open-Source Intelligence Techniques, (Fazlioglu, 2018)

7. **Conduct privacy impact assessments (PIAs):** Perform PIAs to identify and mitigate privacy risks associated with new or existing data processing activities. PIAs help in assessing the impact on individuals' privacy rights and implementing appropriate measures to address any identified risks.
8. **Develop a data policy framework:** Based on the legal advice received, establish a comprehensive data policy framework that aligns with the requirements of GDPR or CCPA. This framework should outline how the county collects, uses, stores, and shares personal data, as well as the measures taken to protect data privacy and security.
9. **Monitor and audit compliance:** Regularly review and monitor data handling practices to ensure ongoing compliance with GDPR or CCPA. Conduct periodic internal audits or engage external auditors to assess the effectiveness of the data policy framework and identify areas for improvement.
10. **Stay informed about regulatory updates:** Keep abreast of any changes or updates to GDPR, CCPA, or other relevant data protection regulations. Maintain a proactive approach to compliance and make necessary adjustments to the county's data policy framework as needed.

Because Curaçao does not have a data policy framework legislation in place, the Country and the institutions that serve at the country's will are extremely vulnerable. There are interventions that can assist Curaçao as a country without a data police. These strategies can work toward the development of the necessary data policy framework legislation.

1. **Alignment and Harmonization:** Strive for alignment and harmonization of data protection regulations to ensure consistency and facilitate cross-border data transfers. This involves assessing the similarities and differences between frameworks and working towards compatible provisions and principles.
2. **Data Transfer Mechanisms:** Establish mechanisms to facilitate the lawful transfer of personal data across borders. For instance, the GDPR provides for various legal transfer mechanisms such as adequacy decisions, standard contractual clauses, binding corporate rules, and derogations. Ensuring compatibility with these mechanisms can promote seamless data flows between countries.
3. **Mutual Recognition:** Explore mutual recognition or equivalency agreements, recognizing each other's data protection frameworks as providing an adequate level of protection. This approach can streamline data transfers and foster trust among countries.
4. **Cooperation and Information Sharing:** Promote cooperation and information sharing among regulatory authorities. This can involve sharing best practices, experiences, and enforcement strategies to enhance the effectiveness of data protection efforts globally.
5. **Privacy Shield Alternatives:** In the case of international transfers involving the European Union (EU), the country should consider alternatives to the EU-U.S. Privacy Shield framework since the Privacy Shield was invalidated by the Court of Justice of the European Union in 2020. Exploring new mechanisms or adopting existing ones, such as standard contractual clauses, can facilitate lawful data transfers between the EU and other countries. (The Consensus Kingdom Law could affect this if implementation begins)
6. **Cross-Border Enforcement:** Establish mechanisms for cross-border enforcement cooperation. This can involve mutual assistance, coordination of investigations, and sharing of enforcement actions. Cooperation between regulatory authorities can deter non-compliant entities and strengthen the enforcement of data protection laws.
7. **Stakeholder Engagement:** Engaging with various stakeholders such as businesses, civil society organizations, and academic institutions can help countries understand different perspectives and gather feedback during the development or amendment of data protection frameworks. This

inclusive approach can contribute to the effectiveness and acceptance of international data frameworks.

8. **Continuous Monitoring and Review:** Regular monitoring and review of international data frameworks are crucial to address emerging challenges, technological advancements, and evolving global privacy expectations. Flexibility and adaptability are essential to ensure that frameworks remain relevant and effective in a rapidly changing digital landscape.



Conclusions and Recommendations

Conclusions and Recommendations

The purpose of this research was to lay out the necessary characteristics and the challenges of becoming a digital society. The aim is to advance the knowledge and skills needed for policy and services development and digital solutions to demonstrate the ways digital engagement works as documented by other countries.

Everything in life is powered by digitalization. There is urgency to ensure that our digital life is safe, and the country makes broad advances in digital development. The economy is being powered more and more by digital solutions and these solutions become the engine of the entire economy and must provide opportunities for all. People are empowered by increasing their inclusion in the digital society and becoming co-creators in a technological nation.

Developing this data maturity is an ongoing process that requires continuous improvement and investment in data-related capabilities. At its best, it involves the collaboration of various stakeholders, including data professionals, IT teams, business units, and leadership, to foster a data-driven culture and maximize the value of data assets.

By delving deeply into the components of *data governance* policies, processes, and standards in place for data collection, storage, quality, security, and privacy and an outlining the well-defined *data strategy* of how data will be used to drive decision-making, innovation, and competitive advantage, it is hoped that the necessary roadmap has been outlined.

The Think To DO Institute research team honed their skills by participating in training from the Nordic Institute for Interoperability Solutions in Estonia. NIIS is the leading developer of country framework solutions. This model articulated *data integration, data analytics and insights, data culture and skills, data privacy and security* policies, procedures and implementation timelining for successful national data policy framework implementation.

As repeated throughout this document, It should be noted that traditional governance models may hinder the agility required to harness the full potential of data. A country's *Data Maturity* is key because it emphasized the need for iterative, collaborative, and adaptive approaches to governance that align with agile development methodologies. The time it takes to realize the framework is contingent upon collaboration efforts and financial prioritization of the country.

Below is the Estonia Integrated National Data Policy Framework that took a decade to fully implement, and which serves as the model for numerous countries, small and large, in the world. It must be noted that it is the model that is being used to design the European Union Data policy framework as mentioned in this document. This framework illustrates the integration of the various topics articulated in the Chapters of this document.

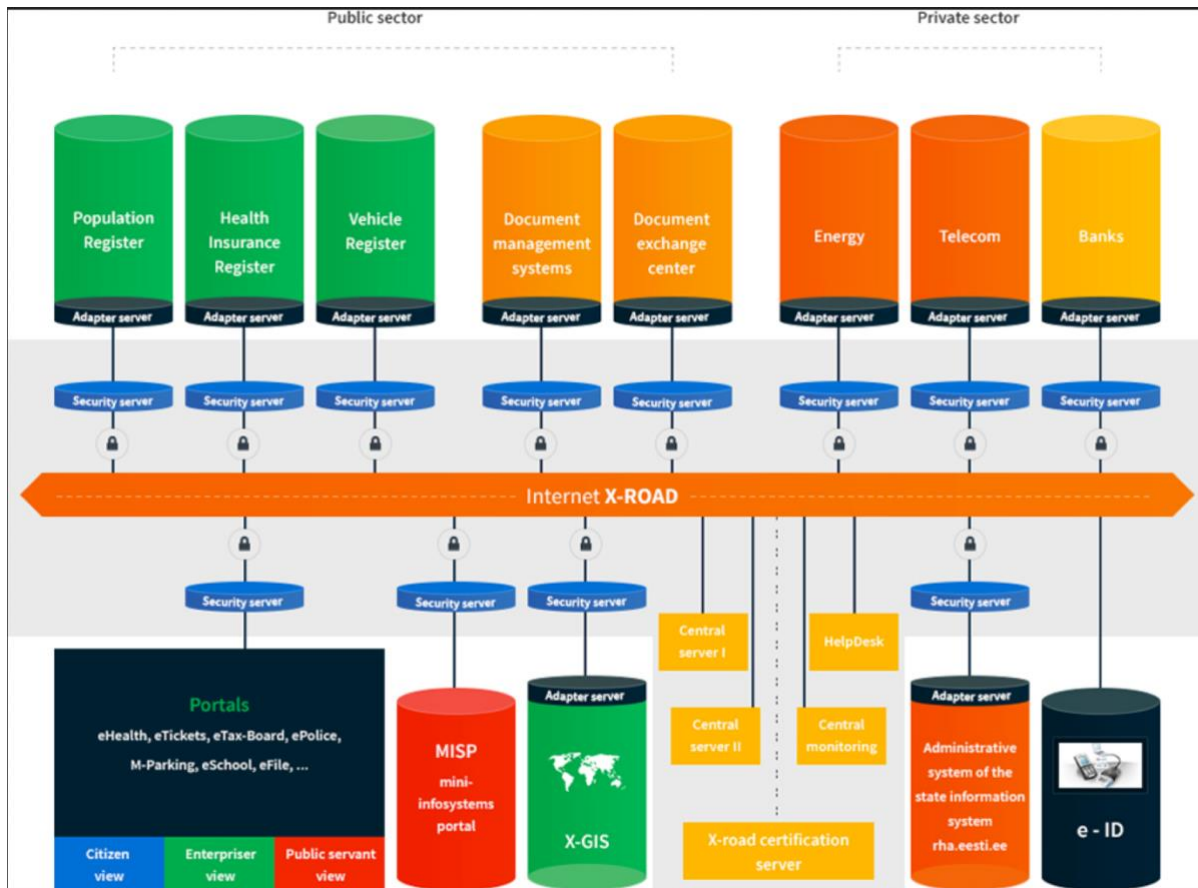


Figure 21: NIIS National Data Policy Framework

In addition to reviewing the best practices of other countries, the various aspects of the following best practices were reviewed within the local private and public institutions. This gave the research the necessary data to determine the maturity level of the local system and those areas that need to be strengthened in order to successfully develop a national data policy framework.

These nine areas of attention create a customer-centered, data-driven community which allows for the safe transfer of data across multiple public and private servers, providing the necessary data sharing to allow for “data-driven decision making” that creates and sustains resilient societies.

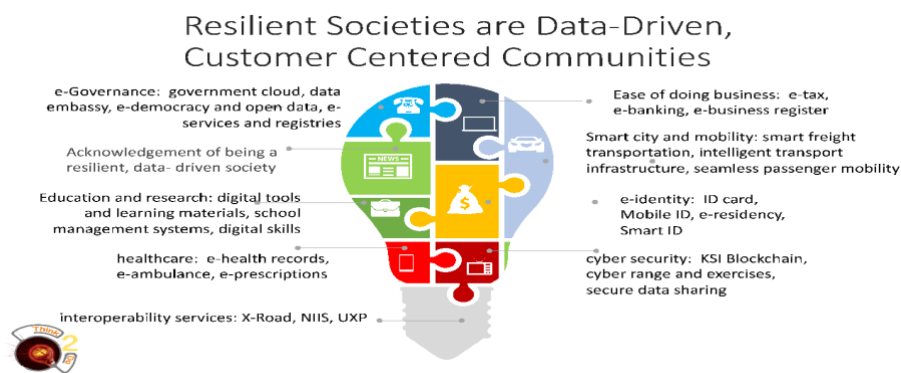


Figure 22: Nine Resilient Society Characteristics enabled by a National Data Framework

Recommendations

As a result of this investigation, it is hoped that Curaçao can further advance toward a resilient, data-driven society. Because of its maturity level, the path to a national data policy framework will take years to fully realize. Statistics are vital for achieving sustainable development goals especially in smaller communities.

The document stresses the necessity of data collection and statistical analysis for effective planning, follow-up, implementation evaluation, and tracking success in attaining international development goals. These actions tend to be more complex in small island communities as it is compounded by their relatively small size, vulnerability, and far greater resource constraints. However, despite the specificities, the only way to really measure progress is to track progress.

Innovations, new tools, and systems to improve data generation and dissemination could potentially help leap-frog statistical challenges. Given the inevitable increase in data demand, statistical systems must balance national, regional, and international requirements, prioritizing statistical development.

As a result of the T2DI research, the following recommendations are offered to expedite the development of and sustainable use of a national data policy framework:

1. Develop together with broad base of public and private stakeholders a consolidated action plan (administrative, legal, technical) needed to make a national data framework implementation successful, with access to all. Include in the plan a monitoring and measurement system to determine the breadth of implementation and success of the framework.
2. More research needs to be performed related to how to reach and sustain data maturity.
3. Research group needs to be broadened and research based on more data points for a small island nation.
4. Adoption and implementation of such a framework can only occur with more education of the users to understand the value of the data-driven, customer-centered community.
5. Government and regulatory bodies should start regulating and providing guidelines for the framework's use by law and by way of work.
6. Government and regulatory bodies should, by example, model transparent behavior in data governance.
7. Establishment of a singular E-identity for all citizens should be implemented as the first structural outcome of the framework because it provides immediate positive results for citizens in their ability to interface with government and receive government services with ease and confidence.
8. After implementing the singular E-identity then next logical structure to provide more positive results for citizens is a "Unified Payment System" or a "Multi-Purpose Payment System". In addition to handling retail transactions, the system is designed to facilitate payments related to government services and utilities, such as taxes, social benefits, fines, and public transportation fees.
9. A unified national data framework is essential to address data gaps in informing policy frameworks and monitoring desired national development outputs and outcomes.
10. A unified national data framework can provide the necessary data to determine the specific laws, policies, processes and programs to drive country resilience and therefore the data needs to be tied directly to the economic and social programs of long- and medium-term goals.

11. Tracking progress and gauging public sentiment can be accomplished by establishing and strengthening partnerships with universities and research institutions to collaborate in data analysis.
12. Adapting the information needs of the international community to the constraints of the island nation is imperative to strike the balance between locally implementable with globally competitive. This can be achieved by educating stakeholders of the positive impact on their organizational outcomes by way of measurement of the socio-economic, educational, and social aspects the data can provide for organizational development and customer services.
13. Enhance collaborations among the small communities, development partners, regional bodies, and technical assistance providers, fostering stronger partnerships to leverage knowledge and resources for the enhancement of statistical systems.
14. Collaboration, mandated by law, across all Ministries to collect and share data internally and externally will lower the costs of data collection, processing, and dissemination within the public sector by systematically utilizing administrative data sourced from existing information systems such as civil registration and vital statistics, health, and education. Supervision related to data exchange will ensure that data is collected once, and used for multiple purposes in a secure and responsible manner.
15. Both the public and private sector must work toward the acceptance of data transparency as it helps to build trust between individuals and organizations, and it can help to prevent misuse or unauthorized access to sensitive information. This includes being transparent about the types of data that are collected, the methods used to collect it, and the purpose for which it will be used.
16. An agreed-upon set of ethical boundaries and concerns to protect privacy, ensure data security, promote fairness, and maintain public trust must be legislated and actualized. By addressing these concerns, governments can establish robust safeguarding measures and guardrails to navigate the complex ethical landscape surrounding data frameworks. These are critical to the success of the national framework.
17. Because Curaçao does not have a data policy framework legislation in place, the country, and the institutions that serve at the country's will, are extremely vulnerable. These strategies and measures increase country resilience while working toward the development of the necessary data policy framework legislation.
18. Understanding public data empowers consumers to make informed decisions. . This knowledge is essential for individuals to take proactive measures to protect their privacy online. Whether it's about choosing products, services, or even political candidates, awareness of public data helps individuals make choices aligned with their preferences and values. In order to form a mutually beneficial data economy, and create trust, companies need to educate users about what the company is doing with consumer data.
19. Lastly, with the increasing reliance on digital platforms, consumer education about public data builds digital literacy, which in turn helps individuals navigate online spaces responsibly, distinguishing between credible and unreliable sources of information. This digital literacy must begin with a digital literacy curriculum in schools and continue through workplace skills, and programs in businesses and in non-profit organizations focused on consumer participation in society.



Glossary

Glossary

Automated failover

Automated failover means (as the term implies) that the backup system takes over automatically when the main system goes down.

Data availability

Data availability is when an organization ensures that all of its business-related data is available to the organization, partners, or end-users at any time of the day, whenever and wherever required.

Data confidentiality

Data confidentiality refers to protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information.

Data integrity

Data integrity is the maintenance of, and the assurance of, data accuracy and consistency over its entire life cycle.

Data interoperability

Data interoperability refers to the ways in which data is formatted that allow diverse datasets to be merged or aggregated in meaningful ways.

Data maturity

Data maturity refers to an organization's ability to effectively manage and leverage data to drive business value.

Data Governance Maturity Model-(Gartner example)

A *data governance maturity model* is by definition a widely used framework and model that organizations and countries can reference to assess and improve their data governance maturity.

While there isn't a single globally recognized standard for a data governance maturity model, there are several widely used frameworks and models that organizations and countries can reference to assess and improve their data governance maturity. Here are a few notable ones:

1. **Capability Maturity Model Integration (CMMI):** CMMI is a well-known model for assessing and improving process maturity in various domains, including data management and governance. While it's not specific to data governance, organizations have adapted the CMMI framework to assess their data governance capabilities.
2. **Data Management Association (DAMA) Data Management Body of Knowledge (DMBOK):** DAMA International provides the DMBOK, which serves as a comprehensive guide to data management practices. The DMBOK includes a maturity model that organizations can use to assess their data management and governance capabilities.
3. **European Data Governance Forum (EDGF) Maturity Model:** The EDGF has developed a maturity model specifically focused on data governance. It provides a framework to assess data governance maturity across multiple dimensions, including strategy, processes, organization, and technology.
4. **Open Data Institute (ODI) Data Maturity Model:** The ODI offers a data maturity model designed to help organizations understand their data practices and improve their data capabilities. While not specific to data governance, it covers various aspects of data management, including governance.
5. **Open Data Charter:** The Open Data Charter is a collaboration between over 170 governments and organizations working to open up data based on a shared set of principles. It promotes policies and practices that enable governments and CSOs to collect, share, and use well-governed data, to respond effectively and accountably to the following focus areas: anti-corruption, climate action and pay equity.
6. **ISO standards for data:** The ISO 27k series are a set of standards, published by the International Organization for Standardization, which provide requirements, guidance, and recommendations for a systematic approach to protect information, in the form of an Information Security Management System (ISMS). (27001, 27002, 27017, 27018, 27701)

ISO 27001 defines the basic requirements for an Information Security Management System (ISMS), and the security controls and security control objectives to be considered for implementation.

ISO 27002 – It provides guidance and recommendations for the implementation of security controls defined in ISO 27001.

ISO 27017 – It provides specific guidance and recommendations for the implementation of security controls in cloud environments.

ISO 27018 – It provides specific guidance and recommendations for the implementation of security controls related to privacy issues in cloud environments.

ISO 27701 – It defines the basic requirements for a Privacy Information Management System (PIMS). Basically, it is ISO 27001 developed to include privacy topics.

ISO 27001 and ISO 27701 are certifiable standards, i.e., organizations can be certified against them by certification bodies, and they provide the basis for continual improvement, which helps keep implemented controls relevant to business objectives and needs and expectations of interested parties, like customers and governments.

ISO 27002, ISO 27017, and ISO 27018 are supporting standards, i.e., they are not certifiable, and only provide best practices for the implementation of controls.

It's important to note that while these models and frameworks provide valuable guidance, organizations and countries may tailor them to suit their specific needs and context. The adoption of a data governance maturity model depends on the specific goals and requirements of the organization or country.

Data Policy Framework

A data governance framework creates a single set of rules and processes for collecting, storing and using data. Even with an ever-growing volume of data, a data governance framework makes it easier to streamline and scale core data governance, maintain policy and regulatory compliance, democratize data.

Data Policy Regulators:

General Data Protection Regulation (GDPR) The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live and outside of the European Union (EU). Approved in 2016, the GDPR went into full effect two years later. Its aim is to give consumers control over their own personal data by holding companies responsible for the way they handle and treat this information. The regulation applies regardless of where websites are based, which means it must be heeded by all sites that attract European visitors, even if they don't specifically market goods or services to EU residents.

California Consumer Privacy Act (CCPA) The California Consumer Privacy Act is a state statute intended to enhance privacy rights and consumer protection for residents of the state of California in the United States introduced in 2018 and which serves as a model for state privacy acts in the United States.

Personal Data Protection Act (PDPA) in Asia/Singapore Singapore's Personal Data Protection Act (PDPA) governs the collection, use, disclosure, and care of personal data, as described in the official Quick Guide to the PDPA. At the core of the PDPA are the 9 Main Data Protection Obligations, which attempt to strike a balance between individuals' rights to protect their personal data and organizations' needs for this data for legitimate and reasonable business purposes. It serves as a model privacy act for Asia.

Brazilian General Data Protection Law (LGPD) The General Personal Data Protection Law, is a statutory law on data protection and privacy in the Federative Republic of Brazil. The law's primary aim is to unify 40 different Brazilian laws that regulate the processing of personal data.

Data by Proxy

Proxy Data are measurements that can be substituted for direct measurements when a direct measurement is not possible.

Digital identity

is typically defined as a one-to-one relationship between a human and their digital presence.

Digital presence

can consist of multiple accounts, credentials, and entitlements associated with an individual.

National Interoperability Framework (EIF)

is a European Union framework which gives specific guidance on how to set up interoperable digital public services. The EIF conceptual model for public services covers the design, planning, development, operation and maintenance of integrated public services at all governmental levels from local to EU level.

External Data

is data generated, collected or processed by a third party, but used supplementary by the company to support business processes. Examples of external data are Market Research, Social Media Data, Economic Indicators and Census data.

Influencer

an approved User of relevant social media, and compliant with the terms and conditions thereof, who meets all the criteria set out in these terms and conditions and who has successfully registered to the Service provided by Hashtag Viral via. the APP, thereby accepting the agreement and including the terms and condition of this document

or

a user on social media who has established credibility in a specific industry with access to a large audience and can be one who can persuade others by virtue of their authenticity and reach.

Internal Data

is data generated, collected or processed by the company itself as a means of supporting its core business. is not restricted to but may include data from Customer Relationship Management (CRM) systems, Transactional Data, Employee Data, Product and Inventory Data etc.

ISO Standards

ISO is an abbreviation of the International Standards Organization. They are an independent body made up of an extensive network of individuals who are experts in different areas. This allows them to share and pool together their experience and knowledge of different fields to determine best practices and key safety information to define the best way of carrying out certain tasks or processes. An ISO standard is essentially an internationally recognized way of doing something. It means that everyone follows the same set of guidelines no matter where they are based, resulting in a safer, more consistent end result. This benefits both the organization and the customer or end user. For companies, they are secure in the knowledge that this standard is followed and recognized worldwide. For customers, they know they are getting a product or service which is safe, good quality and trustworthy.

(Nederlandse Overheid Referentie Architectuur) NORA also known as (Dutch National Interoperability Framework (NIF)

is intended to give direction and to be a supporting instrument for Public Administrations. It contains policy frameworks and arrangements for setting up the ICT systems of the Dutch government. These frameworks and agreements ensure that these ICT systems work well together and make optimal re-use of existing solutions. NORA also provides principles, standards, and building blocks grouped in various themes at operational level

Primary Data

refers to original data that has been generated or collected directly from the source. It is data that is not previously published or processed by others. This could include sales records, customer feedback, or employee surveys.

Secondary Data

refers to data that has already been collected, processed, and published by someone else for a different purpose.

Structured Data

Structured data is data that has a standardized format for efficient access by software and humans alike. It is typically tabular with rows and columns that clearly define data attributes. Computers can effectively process structured data for insights due to its quantitative nature.

Unstructured Data

Unstructured data (or unstructured information) is information that either does not have a pre-defined data model or is not organized in a pre-defined manner. Unstructured information is typically text-heavy, but may contain data such as dates, numbers, and facts as well.



Figures

Figures

- Figure 1: Gartner Data Governance Maturity Model
- Figure 2: Distribution of Curaçao Respondents Data Governance Maturity Survey
- Figure 3: Submarine Cable Map of the Caribbean
- Figure 4: Fixed Broadband Network Speeds 2015
- Figure 5: Households with Shared ICT Computer Access
- Figure 6: Development Planning Process
- Figure 7: Decision-making Tree for Determining Digital Services Security
- Figure 8: CIA Triad
- Figure 9: Comparison of the Common Models of Data Security Systems
- Figure 10: Comparisons of DIE to CIA
- Figure 11: EIF Conceptual Model for Interoperability
- Figure 12: EU Country Overview
- Figure 13: Comparison of Primary and Secondary Data
- Figure 14: Six Dimensions of Data Quality
- Figure 15: Evaluation External Data (McKinsey)
- Figure 16: Data Format/Data Sources Matrix
- Figure 17: Results of Curaçao Openness of Data
- Figure 18: HLS Framework
- Figure 19: Types of Mass Media
- Figure 20: 3Rs: Essential components of Influencer Marketing
- Figure 21: NIIS National Data Policy Framework
- Figure 22: Nine Resilient Society Characteristics Established by a National Data Framework



Resources and Bibliography

Resources

Think Tanks

Centre for International Governance Innovation (cigionline.org)

Gartner (Gartner.com)

Nordic Institute for Interoperability Solutions (NIIS.com)

Open Data Institute (data.org)

World Economic Forum (Strategic Alliance: weforum.org>strategic-intelligence)

Bonnie is Contributor to Agile Governance Workgroup and is Pro Digital Member (Unlimited access to advanced analytics and collaboration tools on the Strategic Intelligence platform)

University Research

UC Berkley (em-exeuctive.berkeley.edu)

Cambridge University (www.cambridge.org.data-and-policy)

Topic: Data protection for the common good:

Topic: Research Data Management Policy Framework

Harvard Data Science Review (hdrs.mitpress.mit.edu)

Non-Regulatory Government Agency

National Institute of Standards and Technology (www.nist.gov)

Topic: Research Data Framework (RDaF)

Unique Government Forums

United Nations CEB (insceb.org)

Topic: Mapping and comparing data governance Frameworks

OECD (OECD.org)

Topic: Digital Government

Topic: Recommendation of the Council on National Digital Security Strategies

Topic: OECD Digital Government Index (DGI): 2019

Bibliography

Collegebescherming persoonsgegevens, Curaçao, 2022.

Data Policy Insight Briefing, World Economic Forum: 2022.

Digital Identity Guidelines, IST Special Publication 800-63-3, US Department of Commerce, June 2017.

"How to Make Your Data Fair", Force11, Utrecht University, 2016.

Landsverordening Bescherming Persoonsgegevens, Curaçao, 2013.

Proxy Discrimination in Data-Driven Systems, CMU, 25 July 2017, <https://arxiv.org/pdf/1707.08120.pdf>

How Discrimination occurs in Data Analytics and Machine Learning: Proxy Variables, Toward Data Science, 5 February 2020 (research summaries)

The Ultimate OSINT Handbook: A Guide to Open-Source Intelligence Techniques, Fazlioglu, 2018.

Kulshrestha, Juhi; Eslami, Motahhare; Messias, Johnnatan; Zafar, Muhammad Bilal; Ghosh, Saptarshi; Gummadi, Krishna P.; Karahalios, Karrie (2019). "Search bias quantification: investigating political bias in social media and web search" (PDF). *Information Retrieval Journal (2019) 22:188–227*. **22** (1–2): 188–227. doi:[10.1007/s10791-018-9341-2](https://doi.org/10.1007/s10791-018-9341-2). S2CID 52059050

Unravelling the Complexities of National Data Exchange Networks, Nordic Institute for Interoperability Solutions, NIIS, March 2023.

Unleashing the Internet in the Caribbean Removing Barriers to Connectivity and Stimulating Better Access in the Region, Curacao, February 2017.

2023 World Press Freedom Index-journalism threatened by fake content industry, Reporters Without Borders(RSF), 2023.

Online Resources:

<https://www.ashineconsultancy.com/2021/04/30/establish-trust-in-your-data-with-master-data-management>
<https://businessoverbroadway.com/2014/07/30/the-what-and-where-of-big-data-a-data-definition-framework/>

<https://www.bridgingpointsmia.com/services/influencer-marketing/>

https://cuatro.simcdn.nl/cbscuracao/uploads/integration_of_ict_in_private_households.pdf?cb=7NdwqBIM

<https://www.dama-nl.org/wp-content/uploads/2020/09/DDQ-Dimensions-of-Data-Quality-Research-Paper-version-1.2-d.d.-3-Sept-2020.pdf>

<https://data.europa.eu/en/news-events/news/open-data-maturity-report-2022-out>

<https://data.europa.eu/en/publications/open-data-maturity/2022#country-overview>

<https://engaiodigital.com/types-of-influencers/>

<https://www.fortinet.com/resources/cyberglossary/cia-triad>

<https://www.hitechnectar.com/blogs/data-governance-maturity-models-explained/>

<https://joinup.ec.europa.eu/sites/default/files/inline-files/Netherlands%20Factsheet%20Validated.pdf>

<https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail>

<https://leverageedu.com/blog/types-of-mass-communication/>

<https://www.lido.app/post/internal-and-external-data>

<https://www.nen.nl/en/managementsystemen/high-level-structure-hls>

<https://www.niis.org/blog/2020/1/20/interoperability-puzzle>

<https://www.submarinemap.com/landing-point/willemstad-curaçao>

<https://www.teksystems.com/list>

<https://www.toppers4u.com/2022/07/primary-data-definition-features.html>