Mozambique Data Governance Strategy and Policy Mapping

Country visit 28 July – 1 August 2025

United Nations Economic Commission for Africa
Prepared by Nnenna Ifeanyi-Ajufo - Project Lead Consultant

Table of Contents

1. Goals and Objectives

The first and most critical phase in developing a National Digital Governance Strategy is the articulation of its foundational goals and objectives. This step involves an intensive stakeholder analysis and diagnostic assessment of the nation's current digital ecosystem, legal infrastructure, institutional capabilities, and socio-political landscape. Here, the primary aim is to establish a clear rationale for implementing digital governance, addressing fundamental questions: What institutional inefficiencies or societal challenges is digital governance intended to resolve? Are we targeting improved public service delivery, enhanced transparency, citizen inclusion, or economic growth through data-driven innovation? These reflections must be translated into SMART (Specific, Measurable, Achievable, Relevant, and Time-bound) objectives that align with national development plans, regional digital transformation agendas (such as the African Union Digital Transformation Strategy), and global frameworks like the UN Sustainable Development Goals. Furthermore, defining the scope at this stage is essential. This includes identifying which data domains health, education, finance, civil registration are of priority, and specifying the institutional boundaries, systems, and jurisdictions that will be initially included. Special attention should be given to the country's legacy systems and the digital divide, ensuring inclusivity and scalability in design.

2. Executive Support and Political Buy-In

The success of any data governance strategy is inextricably tied to sustained political will and executive sponsorship. This stage requires mobilizing support from the highest levels of government typically the Office of the President, along with key cabinet ministries such as ICT, Finance, and Justice. High-level endorsement legitimizes the initiative and ensures that data l governance is not viewed as a technocratic or IT-only project but as a core instrument of statecraft and public sector reform. Here, the task is both technical and rhetorical. One must develop a compelling value proposition that demonstrates how data governance serves national interests enhancing fiscal accountability, reducing corruption, fostering innovation, and attracting foreign investment. Engaging parliamentarians, regulators, civil society, and the private sector through roundtables and policy dialogues creates a participatory momentum. Institutional champions individuals or entities who can influence political and administrative circles should be identified and empowered to steer the agenda forward.

3. Establishing a Data Governance Framework

With executive backing in place, the next phase is the establishment of a formal data governance framework. This framework functions as the operating system for digital governance, setting the institutional architecture and rulebook for how data will be governed across the public sector. It typically involves the creation of a national Data Governance Commission/Council, supported by thematic committees and operational

working groups. These structures should include representatives from key ministries, national statistics offices, regulatory bodies, academia, civil society, and the private sector. Roles must be clearly delineated data stewards to ensure data quality, custodians to oversee technical infrastructure, and data owners within government departments responsible for data lifecycle management. Central to the framework is a national data governance policy, which articulates guiding principles such as data sovereignty, interoperability, ethical data use, and inclusivity. This policy should also define cross-cutting standards for metadata, identifiers, taxonomies, and reference architectures. It is at this stage that legal scholars and policymakers must closely assess the existing legislative framework to identify gaps in data protection, access to information, and cybercrime law, which may need to be revised or developed.

4. Developing Data Policies and Operational Procedures

Once the overarching framework is established, the focus shifts to operationalizing it through robust data policies and procedures. These instruments translate high-level principles into actionable rules and routines. Data policies should comprehensively cover issues such as data classification, anonymization, archival and retention schedules, ethical AI use, and cross-border data flows. This is especially pertinent in East Africa, where regional integration under blocs like the East African Community (EAC) necessitates harmonization of data governance standards. Procedures must be developed for every step of the data lifecycle collection, storage, access, sharing, and disposal with an emphasis on standardization, security, and transparency. Policies must be informed by comparative legal analysis and best practices, ensuring alignment with regional norms like the AU Data Policy Framework and global norms such as the OECD Data Governance Framework and GDPR principles, while also being responsive to local contexts such as the role of customary and indigenous norms in data ownership and data literacy disparities.

5. Implementing Data Quality Management Systems (DQMS)

Ensuring the integrity and utility of public data is a cornerstone of effective digital governance. Therefore, implementing a data quality management system is not merely a technical requirement but a strategic imperative. This phase involves defining metrics for assessing data accuracy, completeness, consistency, timeliness, and relevance. Public institutions must adopt systematic data profiling and cleansing methodologies, while embedding validation rules at the point of data entry. Where data resides in legacy paper-based formats, digitization and optical character recognition (OCR) tools must be deployed with robust audit trails to prevent transcription errors. Furthermore, institutions should implement continuous data improvement loops and citizen feedback mechanisms to detect and correct inaccuracies. Quality assurance mechanisms should also be embedded within e-government platforms, such as civil registration systems, tax portals, and social protection databases, which often serve as primary sources of national datasets.

6. Implementing Data Governance Controls and Cybersecurity Protocols

At this phase, security, privacy, and ethical considerations come to the forefront. As digital government expands, so too do the risks of data breaches, surveillance abuse, and algorithmic discrimination. Therefore, robust governance controls must be enacted to restrict access based on user roles, and to enforce accountability through audit logs, two-factor authentication, and access recertification. A tiered model of data sensitivity should be applied, ensuring that health records, biometric data, and personal identifiers receive higher levels of encryption and access controls. Privacy-by-design principles must be embedded in all digital systems. Additionally, cybersecurity strategies must be closely integrated with data governance, ensuring alignment with the national cyber defense architecture. This includes not only technical firewalls but also legal deterrents such as criminal penalties for unauthorized access, identity theft, or data manipulation.

7. Developing a Data Governance Strategy Roadmap

With foundational components in place, it becomes critical to develop a detailed implementation roadmap. This roadmap should outline phased activities short-term wins, mid-term institutional reforms, and long-term transformational goals each with corresponding timelines, performance indicators, and resource allocations. The roadmap should prioritize interventions based on urgency, feasibility, and strategic impact. For example, digitizing birth and death registration might be prioritized for its utility in planning and social services. Governance mechanisms for this roadmap must include change management strategies, training and capacity-building programs, and mechanisms for inter-agency coordination. Risk assessments and mitigation strategies should also be embedded to deal with political, technical, or financial obstacles that may arise.

8. Monitoring, Evaluating, and Improving the Strategy

Finally, a dynamic monitoring and evaluation (M&E) framework must be established to track progress, measure impact, and adapt the strategy as conditions evolve. This phase involves defining KPIs that reflect not just technical outputs such as the number of digitized records but also developmental outcomes like improved public trust, reduced service delivery time, and increased access to justice. Regular reporting cycles, independent audits, citizen satisfaction surveys, and policy reviews should inform continuous improvement. Institutions should institutionalize learning platforms such as communities of practice and digital innovation labs where insights from implementation are shared, and emerging challenges are collaboratively addressed. Moreover, the strategy must remain adaptive to new technological paradigms, such as AI, quantum computing, and digital identity ecosystems, ensuring that the country remains resilient and sovereign in a fast-evolving global data landscape.

Mozambique National Data Ecosystem Map

1. **Core Components**

Component	Description
Data Producers	Institutions that collect or generate data from primary or administrative sources.
Data Processors	Organizations that analyse, transform, or enrich data.
Data Users	Stakeholders who use data for policy, research, service delivery, or advocacy.
Regulators & Coordinators	Institutions that create and enforce rules on data governance, privacy, and interoperability.
Infrastructure Providers	Entities providing ICT, cloud, internet, and digital services.
Civil Society & Citizens	End-users of digital public services and advocates for data rights.

2. Key Stakeholders by Category

Government (Public Sector)

Institution	Role in Ecosystem
Instituto Nacional de Estatística (INE)	Official statistics producer; key data aggregator and coordinator.
Ministry of Science, Technology and Higher Education (MCTES)	Leads digital transformation and innovation policy.
Ministry of Economy and Finance (MEF)	Uses data for planning, budgeting, and development indicators.
e-Government Agency (INTIC)	ICT policy implementer; manages digital government platforms.
Ministry of Health (MISAU)	Health data collection, HIS, DHIS2 management.
Ministry of Interior	Identity data, civil registration, and security systems.
Central Bank (Banco de Moçambique)	Financial and economic data collection and oversight.

Private Sector & Infrastructure Providers

Entity	Role
Telecommunication companies (e.g. Vodacom, Movitel, Tmcel)	Mobile data, call metadata, digital inclusion data.
Banks & Financial Services	Transaction and digital ID data, fintech integration.
Tech Startups & Data Platforms	Innovation in data visualization, fintech, and service delivery.
Internet Service Providers	Key digital infrastructure players; support cloud/data centers.

Civil Society, Academia & Media

Group	Role
Centro de Integridade Pública (CIP)	Data transparency, anti-corruption watchdog.
Eduardo Mondlane University	Research, policy analysis, data training.
Journalists / Media Houses	Use data for investigative reporting, fact-checking.

UNECA's approach for stakeholder Engagement

1. **Audience:**
    - **Technical/Operational:** Questions about specific technologies, incident response steps, access control mechanisms, etc.
    - **Legal/Compliance:** Specific questions on interpretation of laws, regulatory changes, and compliance frameworks.
    - **End-Users/Citizens (where applicable):** Questions on their experience with data, trust, and expectations of digital services.

2. **Delivery Method:**
    - **Interviews/Workshops for stakeholders:** Given their strategic role, one-on-one interviews or small group workshops using questions are likely more effective than a simple written questionnaire. This allows for follow-up questions, clarification, and building rapport.
    - **Surveys for Broader Stakeholders:** For a wider audience, well-designed detailed questionnaire to efficiently collect data for easier analysis, alongside open-ended fields for qualitative input.

3. **Context and Framing:**
    - **Clear Purpose:** When presenting the questions, clearly articulate *why* this information is being collected and *how* it will be used to build the strategy.

- **Anonymity/Confidentiality:** Assure respondents their answers will be used to inform the strategy and maintain confidentiality where appropriate to encourage candid responses.
- **Pre-reading Material:** Provide a brief, high-level overview of what "data governance" means in this context, perhaps with a few simple examples, to ensure everyone starts from a shared understanding.

4. **Beyond the Questionnaire:**
    - **Document Review:** Complement questionnaires with a review of existing policies, organizational charts, IT infrastructure diagrams, and any past audit reports.
    - **Process Mapping:** Observe or map current data flows for key processes to understand prospects and identify challenges.
    - **Data Quality Assessment (Technical):** If possible, run automated data quality checks on existing digital datasets to objectively assess their current state.
5. **Iteration and Validation:**
    - Use the initial responses to identify common themes, insights, and areas needing deeper exploration.
    - Consider a second round of more targeted questions or follow-up discussions based on initial findings.
    - Validate key findings with a subset of stakeholders to ensure accurate interpretation.

Assessment Questions

To achieve this process there will be two sets of questionnaires. First for the one-on-one stakeholder engagement during the stakeholder engagement/ capacity building week and visit to Mozambique and another one for the broader institutional perspective to be returned after the stakeholder engagement/ capacity building week.

PARTI: One-On-One Stakeholder Engagement- Stakeholder Engagement/ Capacity Building Week

Name
Institution/organization
Sector (Gov't, Private, Civil Society, Academia, etc.)
Role/Title
Level (National / Regional / Local)
Date

1. **General Context and Objectives**

a) What are your institution's main priorities related to data?

b) How do you define "data governance" in your context?

c) What are the key problems or risks you face with data today?

d) What would a successful national data governance framework look like to you?

2. **Data Collection, Use, and Management**

a) What types of data does your institution collect, generate, or manage?

b) Who determines what data is collected, and how is that decision made?

c) What data standards (if any) do you use for quality, format, or metadata?

d) How is data stored and secured? Locally, on cloud, hybrid?

3. **Data Privacy, Security & Ethics**

a) What privacy or data protection regulations apply to your operations?

b) How do you obtain consent or ensure data subjects' rights are respected?

c) Are data subjects informed or asked for consent before data is collected or used?

d) What challenges do you face with cybersecurity or data misuse?

e) Are there ethical guidelines for data collection and sharing?

4. **Data Sharing and Access**

a) How do you share data internally and externally?

b) What legal or institutional barriers limit data sharing between agencies?

c) Who controls access to sensitive datasets?

d) Do you have data-sharing agreements or memorandums of understanding (MoUs) with other entities?

5. **Institutional Roles and Coordination**

a) Who is responsible for data governance in your institution? (Is there a Chief Data Officer or equivalent?)

b) What coordination exists across government departments on data policy?

c) What role do regulators, civil society, or the private sector play in your data ecosystem?

d) How does your institution engage in setting national or sector-specific data standards?

6. **Capacity, Skills, Resources and Infrastructure**

a) Does your team/organization have adequate skills for data management and governance?

b) What training or capacity-building support would you find helpful?

c) Are infrastructure or funding challenges limiting effective data governance?

d) Do you face infrastructure challenges (connectivity, storage, computing power) that affect data governance?

7. **Policy, Legal, and Regulatory Landscape**

a) What laws or policies currently guide data management in your sector?

b) Are there legal gaps or overlaps creating uncertainty in data governance?

c) What upcoming laws or reforms might affect your data-related work?

8. **Inclusivity, Equity, and Use Cases**

a) How do you ensure that data collection and use are inclusive (e.g., gender, minority groups, rural areas)?

b) How do you use data to inform policy or public service delivery?

c) Are there examples where better data governance improved outcomes in your institution?

d) How are citizens or data subjects engaged or informed about how their data is used?

Section 8: Governance Practices

a) Is there a formal policy or guideline on how data is collected, stored, shared, and protected in your institution?

b) Who is responsible for overseeing data governance? Is there a designated data officer or team?

c) Are there internal or external audits or reviews of your data management practices?

Section 9: Vision and Recommendations

a) What does good data governance look like to you?

b) What should be the top priorities in the national Data Governance Strategy?

c) How would you like your institution to be involved in the development or implementation of a data governance strategy?

PART II QUESTIONNAIRE FOR INSTUTIONAL RESPONSE

Name of Institution/Organisation
Sector (Government, Private, Civil Society, Academia, etc.)
Contact Person
Role/Title
Level (National / Regional / Local)
Date

Digital Readiness and Infrastructure

1. What digital systems or platforms (e.g., databases, document management, ERP, CRM) are currently in use within your organization? Please list them.
2. What proportion of your daily operations is conducted digitally versus manually or on paper? (Please estimate as a percentage.)
3. How reliable and up-to-date is your organization's IT infrastructure (computers, servers, networks, internet connectivity)?
4. What are the main barriers to increasing digitalization in your department (e.g., funding, skills, resistance to change, infrastructure limitations)?
5. Is there a formal digital transformation strategy or roadmap guiding your organization's move from paper/manual to digital processes?
6. How would you rate the overall digital literacy and IT skills of your staff? Are there ongoing training programs?
7. How is data currently transferred or shared between departments or agencies (e.g., email, physical transfer, shared drives, cloud services)?
8. Are there secure and reliable backup systems in place for critical digital data? How frequently are backups performed and tested?
9. Are there standardized protocols or APIs for data exchange between digital systems within your organization or with external partners?
10. Is there a centralized IT support team or helpdesk to assist staff with digital tools and infrastructure issues?
11. Are there any critical business processes that cannot currently be digitized? If so, why?
12. What contingency plans or disaster recovery processes exist for digital infrastructure failures?
13. How are software and hardware upgrades managed and funded within your organization?
14. Are there any interoperability issues between the digital systems used by different departments or agencies?
15. What are your top priorities for improving digital infrastructure and readiness over the next 3-5 years?

Data Storage and Formats

1. What are the primary formats used for storing data in your organization (e.g., paper, spreadsheets, databases, PDFs, images, audio/video)?
2. What percentage of your data is stored in physical (paper) versus digital formats?

3. Are there standardized digital formats (e.g., CSV, XML, JSON, DOCX) mandated for different data types? If yes, please specify.
4. Where is digital data stored (on-premises servers, cloud storage, external drives, individual computers)?
5. How is paper-based data stored and organized (filing cabinets, archives, offsite storage)?
6. Are there documented policies or guidelines for the storage of different data types and formats?
7. How is the migration from paper to digital formats managed? Are there ongoing digitization projects?
8. What challenges have you encountered in converting legacy data into modern digital formats?
9. How is metadata (information about the data) stored and managed alongside the primary data?
10. Are there any data compression or encryption practices applied to stored data?
11. How is the storage of large or complex data types (e.g., GIS, multimedia, big data) handled?
12. What is the process for archiving older data, and how is archived data accessed when needed?
13. How do you ensure the security and confidentiality of stored data, especially sensitive or regulated information?
14. Are there regular audits or reviews of data storage practices and formats?
15. What improvements or changes would you like to see in your organization's data storage and format practices?

Data Access and Retrieval

1. Who is authorized to access different types of data within your organization? How are these permissions managed?
2. What systems or tools are used for retrieving data (e.g., database queries, search engines, manual lookup)?
3. How easy or difficult is it for staff to locate and retrieve the data they need for their work?
4. Are there access logs or monitoring systems in place to track who accesses which data and when?
5. How are requests for data access from other departments or external entities handled?
6. What procedures exist for granting, modifying, or revoking data access rights?
7. Are there documented protocols for emergency or time-sensitive data access?
8. How is data retrieval from archived or backup storage managed?
9. What challenges do users face when trying to access data (e.g., delays, incomplete data, lack of search tools)?
10. Is there a central data catalogue or inventory that helps users discover available datasets?
11. How do you ensure that only authorized individuals access sensitive or confidential data?
12. How is the accuracy and timeliness of retrieved data verified?

13. What training or support is available to staff for using data access and retrieval tools?
14. How are requests for new data access or changes to existing access handled and documented?
15. Are there any known bottlenecks or inefficiencies in current data access and retrieval processes?

Data Sharing and Integration

1. What types of data are currently shared internally between departments and externally with other government agencies or third parties?
2. What technical standards or protocols are used to enable data integration and sharing across systems?
3. How frequently is data shared between departments or agencies (real-time, daily, weekly, ad hoc)?
4. What challenges or barriers do you face in sharing data effectively (technical, legal, organizational)?
5. Are there any data silos that prevent effective sharing or integration? If so, what are they?
6. How is data quality maintained when data is shared or integrated from multiple sources?
7. What security measures are in place to protect data during sharing and integration?
8. Is there a centralized data sharing platform or data exchange infrastructure in place?
9. Are there processes for resolving data conflicts or discrepancies arising from integration?
10. What governance structures or committees oversee data sharing and integration activities?
11. How is feedback from data recipients collected and used to improve data sharing?
12. Are there any incentives or mandates encouraging data sharing among departments?
13. How are data sharing risks (e.g., breaches, misuse) identified and mitigated?
14. Is there a strategy or roadmap for improving data sharing and integration capabilities?
15. What future data sharing or integration capabilities would most benefit your organization?

Data Quality Management

For understanding how data accuracy and reliability impact operations and decision-making.

1. How confident are you in the accuracy and completeness of the data your department uses for daily operations and decision-making?
2. Can you recall instances where poor data quality (e.g., outdated, incomplete, incorrect data) led to inefficiencies, delays, or errors in your department's work? Please describe.
3. What impact does unreliable data have on your ability to make informed strategic decisions or allocate resources effectively?
4. Are there specific data sets that you consider absolutely critical for your department's core functions? How is their quality currently ensured?

5. Do you believe that improved data quality could lead to significant cost savings or increased efficiency in your operations? If so, where?
6. How is data quality currently monitored or measured within your department? (e.g., Are there regular checks, or is it mostly reactive when issues arise?)
7. What challenges do your staff face due to inconsistent or inaccurate data?
8. Are there common data quality issues that frequently cause problems (e.g., duplicate records, missing information, inconsistent formatting)?
9. How do you envision a future where you can trust the data available for your decisions? What would that enable?
10. Do existing IT systems support good data quality practices, or do they contribute to data errors?
11. What resources (e.g., training, tools, personnel) do you believe are most needed to improve data quality in your area?
12. In your view, what are the top 2-3 data quality issues that our National Data Governance Strategy must address to achieve real impact?

Lifecycle Management

Understanding how data is managed from creation to disposal, focusing on its value and risk over time.

1. Do you have a clear understanding of how long different types of data are kept in your department, and why?
2. Are there legal or regulatory requirements that dictate how long your department must retain specific types of data? How confident are you in current compliance?
3. What challenges do you face in managing the sheer volume of data accumulated over time (e.g., storage costs, difficulty finding information)?
4. How easy or difficult is it to access historical data when needed for analysis, auditing, or reference?
5. Are there clear guidelines for when data should be archived, deleted, or destroyed? Who makes these decisions?
6. Do you ever find that data you need for current operations is no longer available, or difficult to retrieve, because it was prematurely archived or deleted?
7. Conversely, do you believe your department retains data for longer than necessary, leading to increased storage costs or security risks?
8. How do you ensure that sensitive or personal data is securely disposed of when it is no longer needed?
9. What impact does managing the data lifecycle (from creation to disposal) have on your department's efficiency and resources?
10. Is there a consistent approach to data retention and disposal across all systems and formats (digital and paper)?
11. How do you ensure that valuable data assets are preserved and accessible for future analysis, even if they are no longer actively used?
12. What role does data lifecycle management play in mitigating security risks and data breaches?
13. Do you believe clearer data lifecycle policies would help your department better manage its data assets and reduce risks?
14. How would a more organized approach to data retention and disposal benefit your department? (e.g., compliance, cost reduction, better security).

15. What challenges do you foresee in implementing new, standardized data lifecycle policies across the country?

Security and Privacy

Understanding how data protection and citizen privacy are managed, and the risks associated with breaches.

1. How confident are you that the sensitive data managed by your department is adequately protected from unauthorized access or cyber threats?
2. What level of risk do you associate with a potential data breach involving sensitive citizen or national data? (e.g., financial, reputational, legal, trust).
3. Are you aware of the specific legal and regulatory requirements concerning data privacy that your department must adhere to? How confident are you in current compliance?
4. Have there been any near-misses, incidents, or actual data security breaches (even minor ones) that you are aware of within your department or related entities? If so, what were the consequences?
5. What policies or procedures are currently in place to ensure that personal information is collected, used, and shared only for legitimate purposes, with citizen consent where required?
6. How is staff trained on data security best practices and privacy regulations? Do you believe this training is sufficient?
7. Do you have clear protocols for responding to a data breach, including notification to affected individuals and authorities?
8. What are the primary challenges your department faces in ensuring robust data security and privacy today? (e.g., budget, technology, skilled personnel, outdated systems).
9. How do we ensure that data shared with external partners (e.g., vendors, other agencies) is handled securely and in compliance with our privacy standards?
10. Do you feel there is a clear understanding across government departments about what constitutes "sensitive" data and how it should be handled?
11. What potential impact could a significant data security or privacy failure have on national operations or international relations?
12. How do you balance the need for data sharing and accessibility with the imperative for strong security and privacy?
13. What level of investment in data security and privacy do you believe is necessary to protect our national data assets effectively?
14. How does our current approach to data security and privacy compare to international best practices or other advanced nations?
15. What would success look like for data security and privacy as a result of this strategy, from your perspective?

Data Management Roles and Responsibilities

Understanding who owns, manages, and is accountable for data across the government, fostering clear accountability.

1. Do you believe there is a clear understanding within your department about who is accountable for the quality, security, and integrity of key data assets?
2. Who in your department is currently responsible for making decisions about how data is collected, used, and stored? Is this formal or informal?
3. Do staff members across different functions (e.g., IT, legal, operations) understand their specific roles in managing data effectively?
4. How would you describe the current collaboration between "business" (data users/owners) and "IT" (data custodians/enablers) regarding data management?
5. Are there sufficient human resources and skill sets available to manage your department's data effectively (e.g., data analysts, data stewards, data architects)?
6. What challenges do you face in assigning and enforcing data-related responsibilities?
7. Do you think a dedicated data governance function or committee is needed at a national or departmental level to oversee data policies and standards?
8. How are decisions made regarding investments in data-related technologies and initiatives?
9. How are new data-related projects (e.g., new data collection, system implementations) assessed for their impact on existing data assets and responsibilities?
10. Do you believe that senior leadership has a clear understanding of the importance of data management and their role in championing it?
11. How do we ensure that data management responsibilities are integrated into job descriptions and performance reviews?
12. What incentives could encourage staff to take greater ownership and responsibility for data?
13. What support (e.g., training, tools, clear mandates) would help individuals better fulfil their data-related responsibilities?
14. How will this National Data Governance Strategy help clarify and formalize data management roles and responsibilities across the public sector?
15. What would success look like for data management roles and responsibilities as a result of this strategy, from your perspective?

Mozambique – Data Governance Stakeholder Analysis Matrix Template

Stakeholder	Type (Gov, Private, CSO, etc.)	Role in Data Ecosystem	Interest in Data Governance	Influence / Power	Engagement Strategy
Ministry of ICT	Government	Policy-maker, Regulator	High	High	Strategic partner, involve in policy drafting
National Statistics Office	Government	Data producer	High	Medium	Technical advisor, core working group
Telecom Regulator	Government	Data controller, enforcer	Medium	High	Regulatory alignment meetings
Private Telco	Private Sector	Data generator, service provider	Medium	Medium	Consultation, public-private forum
Civil Society Group (Digital Rights)	NGO	Advocacy, citizen rights	High	Low	Focus groups, community input
Research Institute	Academia	Data analysis, evidence	High	Medium	Policy co-design, technical advisor