Drafting a strategy action plan for the Tibetan authority

Dr. Arvo Ott

Dr. Priit Vinkel

Where Are We Now (AS IS)?

- Key Findings
- Links to other Strategies
- Performance Baseline 2022

eGA.ee

Where Do We Want to Go?

1. Vision
2. Mission
3. Long-term Outcomes 2030
4. Timing
5. Stakeholders

- **Main principles**

- **How Are We Going to Get There?**

Key Actions

1. Digitalization and digitization
2. Metadata/assets management
3. Secure data exchange
4. eID, digital signatures
5. Regulation and ICT architecture
6. Coordination and management
7. People and competences

eGA.ee

Key Sectors Digitalization

1. Population data management and eRegistration in Elections
2. Education
3. Healthcare and welfare
4. eCabinet, eParliament
5. Culture and language
6. Financial Sector, budgeting
7. Digital document management and archiving
8. Geographic Information Systems and land records
9. Human Resource Management

eGA.ee

What resources will be required?

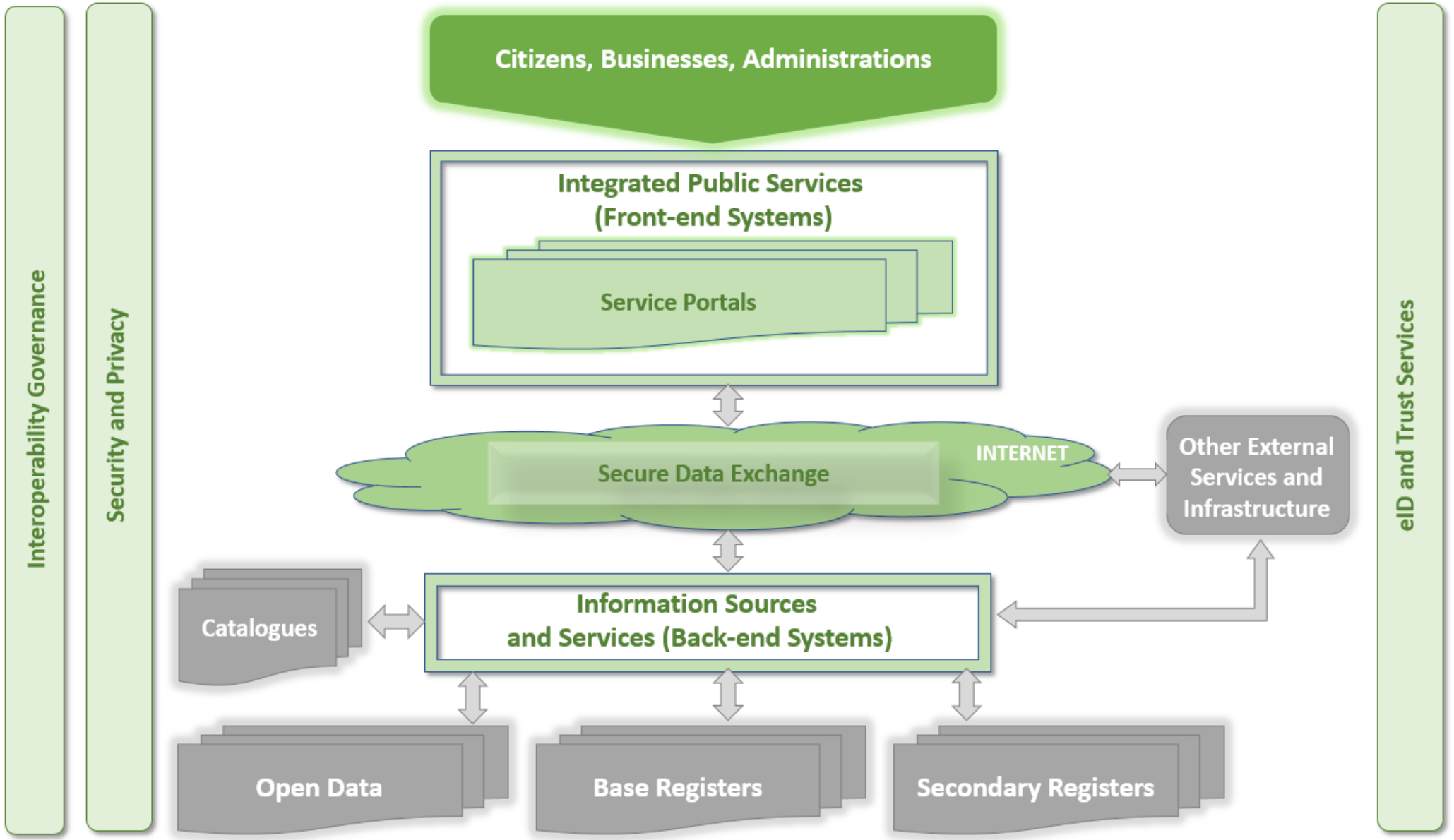
1. Funding sources
2. People
3. Time

eGA.ee

How we will know when we have arrived?

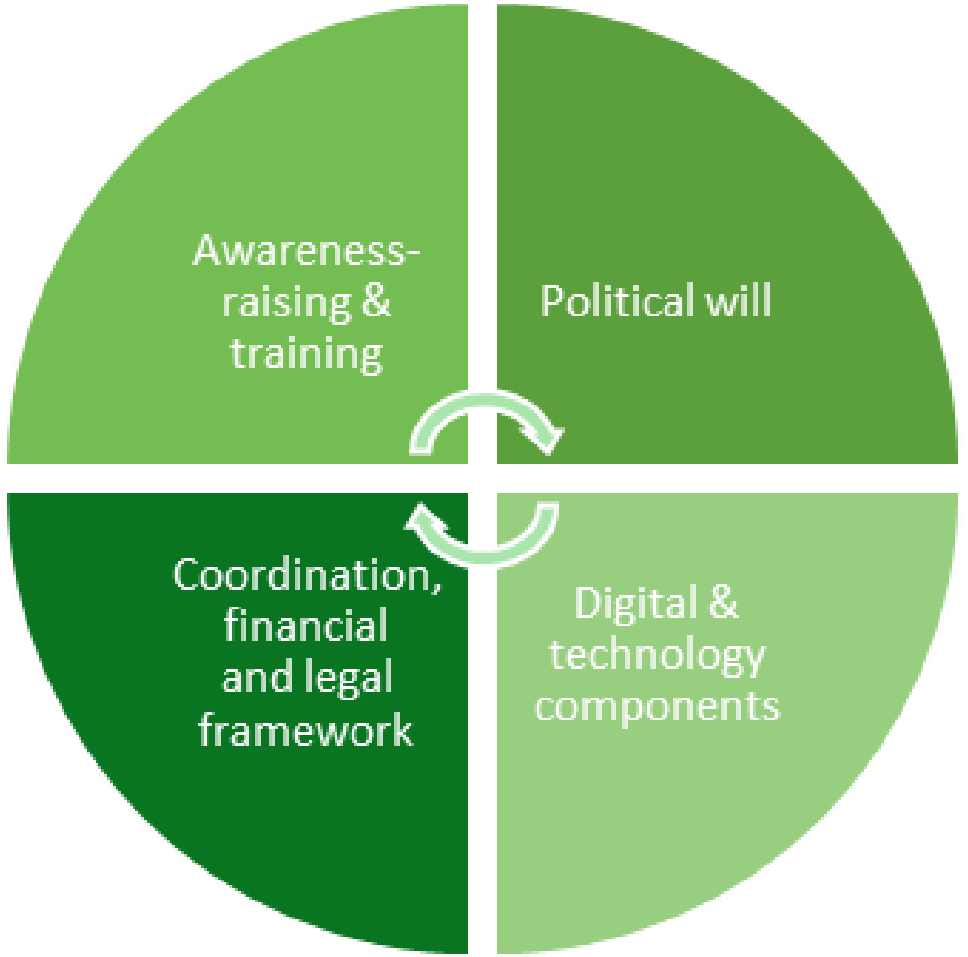
1. Monitoring and evaluation framework
2. Key Performance Indicators
3. Future planning process

Conceptual model of integrated e-governance



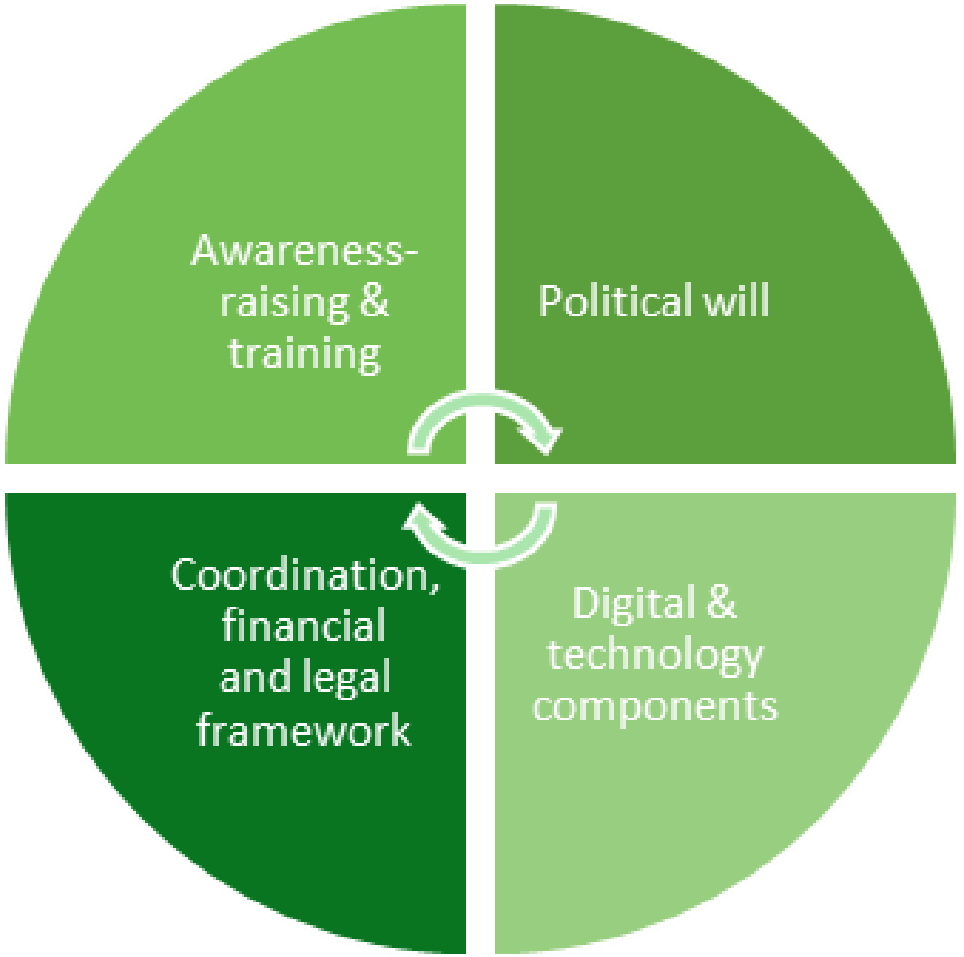
Enablers of e-governance (I)

- **Political will** includes ensuring high-level political leadership that leads to the adoption and implementation of relevant policies and agendas. The introduction of e-governance should be a political priority and political will must be declared at the highest possible level. For this to have proper effect, it is important to identify roles and determine responsibilities for coordination and implementation, encouraging **public-private partnership** and cooperation with **academia**.
- The main **digital and technology components** of e-governance include digital databases and unique identifiers for persons together with electronic ID, secure data exchange, service portals and other building blocks.
- While **infrastructure**, **connectivity** and **affordability of ICT** are relevant concerns when developing digital governance, its implementation is not primarily focused on technology.



Enablers of e-governance (II)

- **Organisational and regulatory issues** are often even more important. A new digital mind-set is needed to fully benefit from modern digital technologies: digital data and transactions need to have legal meaning, data must be reused within government, and service delivery processes need to be redesigned.
- Technology must be integrated into government processes in a **sustainable** way with proper institutional and legislative support, including training of personnel. Otherwise, there will be only few services in place, which leads to a vicious circle, as e-governance will be seen as ineffective, and it may take years to convince government departments and their legal offices or citizens to use the technology.
- High-level coordination of e-government activities among the various government departments is crucial. There must be a **coordinating institution** in place responsible for strategic planning, with a mandate to take (or coordinate) decisions on e-governance for the administration. Standards, policies, and regulations are needed to exchange and reuse data and implement digital identity. Investments in ICT infrastructure and solutions must be monitored to avoid duplication by different institutions.
- In parallel, citizens should be engaged and trained. For successful e-governance, the involvement of civil society and citizens should be encouraged. This is a part of the process of **awareness-raising** about the digital society and general computer literacy development. However, training and awareness-raising are equally important for government staff.



Main building blocks of e-governance (I)

Digital identity and electronic identification

- Trust is a crucial element that enables information society. Both citizens and organisations must be sure that they know the other party they are interacting with. As the delivery of e-services takes place in the digital world, a **digital identity** must be established, and the systems must be implemented for digital identity verification. In parallel with digital identity, digital signatures would be needed – for that, relevant legal, organisational and technical environments need to be developed.
- The main challenge of introducing digital identity, or **electronic identification** is at the conceptual level – there needs to be a **single and unique identifier of persons** in place. The infrastructure for digital identification has to provide for different relevant services, including signing, encryption, sealing, timestamping, certificates validation etc.
- This would require **digitization of the database of population data** and **digitalization of its related procedures**. The digitization of historic data is key. The fact that new birth certificates as well as digitised old entries have unique numbers would offer a good basis for the future provision of eID. In parallel with digital identity, a **digital signature framework is needed**. The main preconditions for the implementation of digital signature are basically the same as for the implementation of a strong digital identity.

Main building blocks of e-governance (II)

Interoperability and secure data management/data exchange

Citizen-centred state and service-oriented information system necessitate linking information systems into an integrated and logical complex. To realize it, different organisations and information systems must be **interoperable**, or in other words, they must be able to work and interact with each other.

- **Secure data exchange** (including a robust **cyber security framework**) is one of the main needs and priorities in e-government development. A central citizen portal (or digital service portal) would be crucial in any service development and dissemination. Government websites need to be at least partly harmonized and equipped with information about services and responsible institutions.
- Among the most important components are also **base registries**, which are reliable sources of basic information on entities such as persons, companies and real estate.
- **Data quality** has to be provided**.** There must be a guarantee that data, issued by public administrations is quality data with legal value.
- **Data security and personal data privacy** should guarantee that information collected about individuals is used only for purposes for which it was originally supplied. Also, citizens and businesses must be assured that they interact with public administrations in an environment of trust and in full compliance with relevant regulations.