

# Digital Government and Transformation



## KEY TOPICS

**Infrastructure sharing for expanding broadband**

**Advantages of infrastructure sharing across sectors.**

**Approaches for regulation and major business models**

**Fair competition among sectoral operators.**

**Broadband network as a 'common utility'.**

**Various models of cross-sectoral sharing.**

**Cooperation and collaboration among the sectoral players.**

## Digital Government and SDGs

There has been a quantitative and qualitative shift in the use of digital technologies in our everyday lives. Our ability to store, compute, and communicate digital data has increased exponentially. Governments are increasingly using digital technologies to improve governance in different areas such as health, education, livelihood, public order, finance, business regulation, tax collection, etc. Recognizing the opportunities provided by digital government, multilateral and bilateral development agencies have actively engaged in research, policy advocacy, and evaluation on many aspects of digital government.

While digital government projects have had positive impacts, there also remains a significant gap between expected and actual benefits. Many projects have failed either partially or fully in achieving the intended objectives with considerable time and cost overruns. The United Nations Committee of Experts on Public Administration (CEPA) has developed a set of governance principles for sustainable development. These values of inclusiveness, accountability, and effectiveness should also guide the design and use of digital government applications.

Digital government applications can contribute to greater effectiveness in governance through improved competency, sound policymaking and collaboration. Inclusiveness has been and continues to be a key concern of sustainable development. Care must be taken to ensure that the use of digital technologies does not lead to further exclusion. The concept of bridging the digital divide has now been broad-



**Good Governance Values aligned to SDGs**

ened to ensure inclusiveness, which includes digital literacy, user-centered design, civic technologies and participatory design. Accountability is a key pillar of democratic governance. Digital government applications, if thoughtfully designed, can enhance the accountability of government to citizens by enhancing transparency and by providing grievance redressal mechanisms.

## Design Approaches for Digital Government

The assumptions generally made while designing and using digital technology point to two predominant misconceptions, namely that technology will automatically lead to better outcomes (technological determinism) and that technology is a neutral tool. The social shaping of technology approach, especially in addressing governance challenges, which are “complex” and “wicked”, is increasingly gaining salience. A plurality of views needs to oc-

cupy prominence in digital technology designs.

Using a participatory approach in the creation of digital government technologies can facilitate a shift in the design and development approach towards co-creation to enhance stakeholder value. Agile methodology is a new entrant in the field of software development and has gained widespread acceptance, especially in addressing the complex socio-technical challenges of governance.

Governments are also adopting a design thinking approach to address public policy problems, including digital government. Design thinking is a nonlinear, iterative process that seeks to understand users, challenge assumptions, redefine problems, and create innovative solutions to prototype and test. The human-centered design approach begins with a deep understanding of the problem context from the user’s perspective. Building a deep empathy with the people for whom the design is being done is central to a human-centered design approach. These approaches to digital technology design, if appropriately adopted, can ensure that digital government applications further the values of inclusiveness, accountability, and effectiveness in governance.

### Design Thinking Framework



Source: <https://www.unssc.org/news-and-insights/blog/power-innovation-and-design-thinking-implementing-2030-agenda-sustainable/>

# Digital Government Strategies

Digital government must not use piecemeal approaches but must be guided through a long-term digital government strategy. The three main components of such a digital government strategy include digital infrastructure, digitally enabled services and human and institutional capacities. While there has been a quantitative leap in access to digital infrastructure, challenges continue to persist. There are geographic and social disparities in access to digital infrastructure. Universal Service and Access Funds (USAFs) and provisioning of public access can bring about greater access to digital infrastructure.

Digitally enabled government services can benefit from a whole-of-government approach (WoG). It implies greater coordination among different layers of government and between various departments of government to provide unified service delivery to citizens. A WoG approach might lead to buck-passing behind the digital veil. Thus, care must be taken to ensure accountability within the government. Digital government applications can also open up new avenues for collaboration with the citizens. E-participation has a long history in participatory development. However, participation should not be reduced to tokenism. Open Government Data (OGD) initiatives and social media can foster greater collaboration with citizens.

Digital government requires a special set of skills and competencies for diverse actors, including citizens and officials. Developing a digital government strategy requires understanding a country's history, social norms, values, beliefs, attitudes and national perceptions surrounding digital technologies. Digital government strategy requires the government to encourage knowledge production and innovation in multiple disciplines such as public administration, management, political science, sociology, anthropology, psychology, economics, and law apart from the traditional computer science domain. A digital government project design and implementation require project management skills such as procurement, finance, testing, quality assurance and maintenance. Governments must also enhance their capacity for continuous monitoring, evaluation, and improvement.

A whole-of-government approach must encourage the flow of data and functions across different government tiers and departments. Thus, interoperability must be encouraged through open Application Programming Interfaces (APIs) and open data standards. Regulations to protect the privacy of citizens in the digital government and digital economy are of utmost importance. Cybercrime refers to such technology-mediated criminal activities that cause intentional harm to individuals, organizations, and society. A digital government strategy needs to address cybercrime proactively to fully benefit from digital technology's potential power for both economic growth and social development.

## Digital Government Project Phases



# Digital Government Project Lifecycle

Digital government applications have been widely used in multiple domains such as urban governance, law enforcement, the judicial system, education, healthcare, agriculture, tax administration, and government procurement. Digital government projects often fail due to poor planning and project management. To prevent such failures, governments need to adopt sound project management practices.

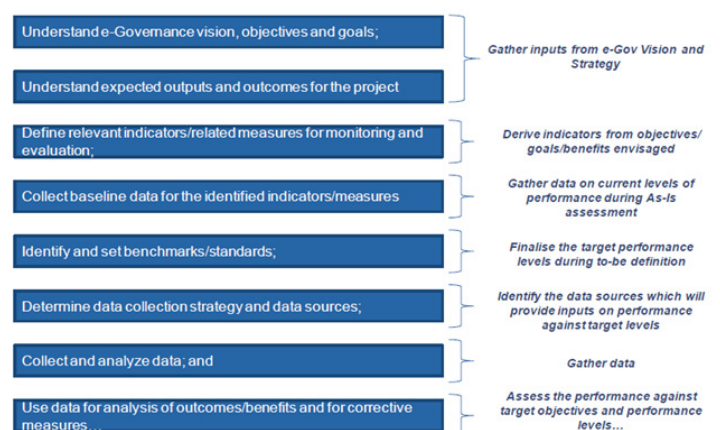
An important consideration in a digital government project is project conceptualization, i.e., identifying the problem or the opportunity for the users that digital technology seeks to address. Mapping the current state, the future desired state and the anticipated performance improvements are vital to the success of a digital government project. In the implementation phase, there are two key considerations – procurement and financing. Project implementers can either develop the application in-house or procure it from an external vendor. Furthermore, off-the-shelf products can be procured when appropriate, as this saves project costs and time. If the requirements do not match, then bespoke development can be procured. Governments must prioritize open-source software to prevent vendor lock-ins. While considering the financing options, governments must budget for the “total cost of ownership” upfront, which accounts for the initial costs of acquisition and operational costs over time. The key options available are public financing, private financing, and Public-Private Partnership financing.

Project development concerns itself mainly with ensuring that the software application is developed within the planned time and cost while ensuring its quality. Project deployment refers to the project going “live” into the user environment. Deployments tend to disrupt the existing process flows. Thus, governments can either

choose to adopt an incremental approach to deployment (i.e., a phased rollout) or adopt a big bang approach and deploy the digital government applications at once.

Monitoring and Evaluation processes help clarify underlying factors affecting the performance, unearth any unintended consequences (positive and negative) and recommend actions to improve performance in future projects/programs. This can be done by establishing Key Performance Indicators (KPIs). Participatory evaluations, involving deeper engagement with the stakeholders, can be considered for increased responsiveness. Concerns of financing can be addressed through a mix of approaches including Whole-of-Government volume sourcing, dynamic procurement, use of Free and Open-Source Software (FOSS), Cloud-based services and most important of all, a realistic assessment of promises and limitations of digital government projects.

## A Monitoring and Evaluation (M&E) Framework



Source: National Institute for Smart Government, Government of India

# Emerging Trends and Way Forward

Fast-paced digitization of government functions and our daily lives has led to “datafication,” which refers to a technological trend turning many aspects of our life into data, often in machine-readable formats. Datafication and the associated “big data” are perceived as a disruptive force in all spheres of our everyday life. Digital data is thus often referred to as the new oil of the fourth industrial revolution. An integral part of this emergent industry 4.0 is the pervasive use of Artificial Intelligence (AI) by the government and the industry. These trends have implications for governments as well. Governments have the role of producers, consumers, custodians, and regulators of digital data.

As governments and citizens increasingly engage in the digital medium, there is a need to identify, authenticate, and authorize citizens digitally. Therefore, governments are investing in providing digital identities to citizens to ensure seamless interaction between citizens and different government entities. We discuss the potential as well as safeguards to be put in place in a digital identity system.

Digital data is a highly valuable resource in the digital economy. The whole-of-economy approach extends the flow of data and services between government and private players through data registries and APIs. While digital data flows can contribute to innovation and economic growth, it must be based on data governance frameworks with strong legislation to prevent the misuse of personal data. EU’s General Data Protection Regulation (GDPR) serves as a useful guide in this respect. The data governance framework must also address concerns around non-personal data. Governments often allow

public access to government-held non-personal data through open data initiatives. However, the private sector’s non-personal data must also be regulated to ensure a level-playing field in the data economy and improve competitiveness.

Artificial intelligence (AI) technologies are being considered a potential game-changer in the digital space. AI systems are being adopted by governments to improve the effectiveness of policymaking and service delivery. Nevertheless, the use of AI systems, if not properly thought, might also dilute the values of effectiveness, inclusiveness, and accountability. There is, therefore, a need for ethical, human-centered and trustworthy designs of AI applications.

### IEEE’s Ethically-aligned Design Principles for Artificial Intelligence

